Kaspersky Internet Security 2013

MANUAL DO USUÁRIO

VERSÃO DO APLICATIVO: 13.0

Prezado usuário,

Obrigado por escolher nosso produto. Esperamos que esse documento ajude você a trabalhar e lhe forneça respostas para esse produto de software.

Atenção! Este documento é propriedade da Kaspersky Lab ZAO (também chamada de Kaspersky Lab): todos os seus direitos são reservados pelas leis de direitos autorais da Federação Russa e por tratados internacionais. A reprodução e distribuição ilegais deste documento ou de partes dele resultarão em responsabilidades civis, administrativas ou criminais, de acordo com a legislação aplicável.

Qualquer tipo de reprodução ou distribuição de qualquer material, incluindo sua tradução, é permitido somente através da permissão por escrito da Kaspersky Lab.

Esse documento, e as imagens com ele relacionadas, somente podem ser usadas para efeitos informativos, não comerciais e pessoais.

A Kaspersky Lab reserva-se o direito de alterar este documento sem notificação adicional. Você poderá encontrar a versão mais recente deste documento no site da Kaspersky Lab, em http://brazil.kaspersky.com/downloads/documentacao.

A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou precisão do material usado neste documento cujos direitos são de propriedade de terceiros, ou por possíveis danos associados ao uso desses documentos.

Data de revisão do documento: 16/5/2012

© 2012 Kaspersky Lab ZAO. Todos os direitos reservados.

http://www.kaspersky.com
http://support.kaspersky.com

ÍNDICE

SOBRE ESTE MANUAL 6
Neste manual 6
Convenções da documentação 7
FONTES DE INFORMAÇÕES SOBRE O APLICATIVO 9
Fontes de informações para pesquisas independentes 9
Discutindo os aplicativos da Kaspersky Lab no fórum 10
Entrando em contato com o Departamento de vendas 10
Entrando em contato com o Departamento de Localização e Escrita Técnica por email 10
KASPERSKY INTERNET SECURITY 11
Novidades 11
Kit de distribuição 12
Principais recursos do aplicativo 12
Serviços para usuários 14
Requisitos de hardware e software 14
INSTALANDO E REMOVENDO O APLICATIVO 15
Procedimento de instalação padrão 15
Etapa 1. Pesquisar uma versão mais recente do aplicativo 16
Etapa 2. Iniciando a instalação do aplicativo 16
Etapa 3. Examinando o contrato de licença 16
Etapa 4. Declaração sobre coleta de dados do Kaspersky Security Network 16
Etapa 5. Instalação 17
Etapa 6. Concluir a instalação 17
Etapa 7. Ativando o aplicativo 17
Etapa 8. Registrando um usuário 18
Etapa 9. Concluindo a ativação 18
Atualizando a versão anterior do Kaspersky Internet Security 18
Etapa 1. Pesquisar uma versão mais recente do aplicativo 19
Etapa 2. Iniciando a instalação do aplicativo 19
Etapa 3. Examinando o contrato de licença 20
Etapa 4. Declaração sobre coleta de dados do Kaspersky Security Network 20
Etapa 5. Instalação 20
Etapa 6. Concluir a instalação 21
Cenários de instalação diferentes do padrão 21
Removendo o aplicativo 21
Etapa 1. Salvar dados para uso futuro 22
Etapa 2. Confirmando a remoção do aplicativo 22
Etapa 3. Removendo o aplicativo. Concluindo a remoção 22
LICENÇA DO APLICATIVO 23
Sobre o Contrato de Licença do Usuário Final 23
Sobre a licença 23
Sobre o código de ativação 24
Sobre o fornecimento de dados 24
SOLUCIONANDO TAREFAS TÍPICAS 26
Ativando o aplicativo 27

Comprando e renovando uma licença ... 28
Gerenciando notificações do aplicativo ... 28
Avaliando o status de proteção do computador e solucionando problemas de segurança ... 29
Atualizando bancos de dados e módulos do aplicativo ... 30
Verificar as áreas críticas do computador quanto à presença de vírus ... 30
Verificação completa do computador quanto à presença de vírus ... 30
Verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus ... 31
Verificando objetos provavelmente infetados ... 32
Restaurando um arquivo excluído ou desinfetado pelo aplicativo ... 32
Recuperando o sistema operacional após infecção ... 33
Verificando email e filtrando anexos em mensagens de email ... 35
Bloqueando email indesejado (spam) ... 36
Verificar o computador quanto à presença de vulnerabilidades ... 36
Processando aplicativos desconhecidos ... 36
Verificar a reputação do aplicativo ... 37
Controlando atividades de aplicativos no computador e na rede ... 38
Protegendo dados particulares contra roubo ... 39
Proteção contra phishing ... 40
Teclado Virtual ... 40
Proteção da inserção de dados com o teclado do computador ... 43
Banca Segura ... 44
Limpeza de Dados Particulares ... 45
Avaliando o status de segurança de um site ... 47
Bloqueando o acesso a sites de várias regiões ... 47
Aplicando o Controle para Pais a usuários do computador ... 48
Configurando o Controle para Pais ... 49
Exibindo o relatório de atividade de um usuário ... 49
Usando o Perfil de Jogo para modo de tela inteira ... 50
Criar e usar o Disco de Recuperação ... 50
Criando um Disco de Recuperação ... 50
Inicializando o computador com o Disco de Recuperação ... 52
Protegendo por senha o acesso ao Kaspersky Internet Security ... 53
Pausando e reiniciando a proteção do computador ... 54
Exibindo o relatório de operação do aplicativo ... 55
Restaurar as configurações padrão do aplicativo ... 55
Importando as configurações do aplicativo para o Kaspersky Internet Security instalado em outro computador ... 58
Usando o Kaspersky Gadget ... 58
A participação na Kaspersky Security Network (KSN) ... 60
Ativando e desativando a participação no Kaspersky Security Network ... 60
Verificando a conexão com a Kaspersky Security Network ... 61
ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO ... 62
Como obter suporte técnico ... 62
Suporte técnico por telefone ... 62
Obtendo suporte técnico através da Minha conta Kaspersky ... 63
Usando o arquivo de rastreamento e o script do AVZ ... 64
Criando um relatório de estado do sistema ... 64
Enviando arquivos de dados ... 65

Execução do script do AVZ 66
GLOSSÁRIO 67
KASPERSKY LAB ZAO 73
INFORMAÇÕES SOBRE CÓDIGO DE TERCEIROS 74
AVISOS DE MARCAS REGISTRADAS 74
ÍNDICE 75

SOBRE ESTE MANUAL

Esse documento é o Guia do Usuário do Kaspersky Internet Security.

Para o uso apropriado do Kaspersky Internet Security, é necessário estar familiarizado com a interface do sistema operacional que você usa, lidar com as principais técnicas específicas desse sistema, saber como trabalhar com email e com a Internet.

Este Manual destina-se ao seguinte:

- Ajudá-lo a instalar, ativar e usar o Kaspersky Internet Security.
- Assegurar a pesquisa rápida de informações sobre problemas relacionados ao aplicativo.
- Descrever outras fontes de informações sobre o aplicativo e formas de receber Suporte Técnico.

NESTA SEÇÃO

Neste manual 6

Convenções da documentação 7

NESTE MANUAL

Este manual contém as seguintes seções.

Fontes de informações sobre o aplicativo

Esta seção descreve as fontes de informações sobre o aplicativo e lista os sites que podem ser usados para discutir a operação do aplicativo.

Kaspersky Internet Security

Esta seção descreve os recursos do aplicativo e fornece informações resumidas sobre as funções e os componentes do aplicativo. Você saberá os itens que estão incluídos no kit de distribuição e os serviços que estão disponíveis para usuários registrados do aplicativo. Esta seção fornece informações sobre os requisitos de software e hardware que um computador deve atender para permitir a instalação do aplicativo pelo usuário.

Instalando e removendo o aplicativo

Esta seção contém instruções passo a passo para instalação e remoção do aplicativo.

Licença do Aplicativo

Esta seção fornece informações sobre os termos gerais relacionados à ativação do aplicativo. Leia esta seção para saber mais sobre a finalidade do contrato de licença, os tipos de licença, as formas de ativação do aplicativo e a renovação da licença.

Solucionando tarefas típicas

Esta seção contém instruções passo a passo para executar tarefas de usuário comuns que podem ser realizadas no aplicativo.

Entrando em contato com o Serviço de Suporte Técnico

Esta seção fornece informações sobre como entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

Glossário

Esta seção contém uma lista de termos mencionados na documentação e suas respectivas definições.

Kaspersky Lab ZAO

Esta seção fornece informações sobre a Kaspersky Lab.

Informações sobre código de terceiros

Esta seção fornece informações sobre os códigos de terceiros usados no aplicativo.

Avisos de marcas registradas

Esta seção exibe marcas registradas de fabricantes terceiros que foram usadas no documento.

Índice

Nesta seção, é possível localizar rapidamente as informações desejadas no documento.

CONVENÇÕES DA DOCUMENTAÇÃO

O texto do documento é acompanhado por elementos semânticos aos quais é aconselhável dar muita atenção: avisos, sugestões e exemplos.

São usadas convenções no documento para realçar os elementos semânticos. A tabela seguinte exibe as convenções do documento e os exemplos do seu uso.

Table 1. Convenções da documentação

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Observe que...	Os avisos são realçados com a cor vermelha e mostrados em caixas. Os avisos fornecem informação sobre possíveis ações indesejadas que podem levar à perda de dados, falhas no funcionamento do equipamento ou em problemas no sistema operacional.
É recomendável usar...	As observações são mostradas em caixas. As notas podem conter sugestões úteis, recomendações, valores específicos para configurações ou casos especiais importantes no funcionamento do aplicativo.
Exemplo: ...	Os exemplos são exibidos sobre fundo amarelo sob o título "Exemplo".

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Atualização significa... Ocorreu o evento *Bancos de dados desatualizados*.	Os seguintes elementos semânticos são exibidos no texto em itálico: • Termos novos • Nomes de status e eventos do aplicativo
Pressione **ENTER**. Pressione **ALT**+**F4**.	Os nomes de teclas do teclado são exibidos em negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de + (adição) indicam o uso de uma combinação de teclas. Essas teclas devem ser pressionadas simultaneamente.
Clique no botão **Ativar**.	Os nomes de elementos da interface do aplicativo, como campos de entrada, itens de menu e botões são exibidos em negrito.
➧ *Para configurar a programação da tarefa:*	As frases introdutórias de instruções são exibidas em itálico e acompanhadas de um sinal de seta.
Na linha de comandos, insira help. Em seguida, a seguinte mensagem será exibida: Especifique a data no formato dd:mm:aa.	Os seguintes tipos de conteúdo de texto são exibidos com uma fonte especial: • Texto da linha de comando • Texto de mensagens que o aplicativo exibe no ecrã • Dados que o usuário deve inserir.
<Nome de usuário>	As variáveis são colocadas entre colchetes angulares. Em vez da variável, insira o valor correspondente, sem os colchetes angulares.

FONTES DE INFORMAÇÕES SOBRE O APLICATIVO

Esta seção descreve as fontes de informações sobre o aplicativo e lista os sites que podem ser usados para discutir a operação do aplicativo.

Você pode selecionar a fonte de informações mais adequada de acordo com o nível de importância e a urgência do problema.

NESTA SEÇÃO

Fontes de informações para pesquisas independentes 9

Discutindo os aplicativos da Kaspersky Lab no fórum 10

Entrando em contato com o Departamento de vendas 10

Entrando em contato com o Departamento de Localização e Escrita Técnica por email 10

FONTES DE INFORMAÇÕES PARA PESQUISAS INDEPENDENTES

Você pode usar as fontes de informação seguintes para realizar pesquisas por sua conta:

- A página do aplicativo no site da Kaspersky Lab
- A página do aplicativo no site do Suporte Técnico (Base de Dados de Conhecimento)
- Ajuda online
- Documentação

Se você não conseguir encontrar uma solução para seu problema, recomendamos que entre em contato com o Suporte Técnico da Kaspersky Lab (consulte a seção "Suporte Técnico por telefone" na página 62).

É necessário ter uma conexão com a Internet para usar fontes de informação no site da Kaspersky Lab.

A página do aplicativo no site da Kaspersky Lab

O site da Kaspersky Lab apresenta uma página individual para cada aplicativo.

Em uma página (http://www.kaspersky.com/kaspersky_internet_security), é possível exibir informações gerais sobre o aplicativo, suas funções e seus recursos.

A página http://brazil.kaspersky.com contém um link para a Loja Virtual. Nela, você pode comprar ou renovar o aplicativo.

A página do aplicativo no site do Suporte Técnico (Base de Dados de Conhecimento)

A Base de Dados de Conhecimento é uma seção no site do Suporte Técnico que fornece recomendações sobre o uso de aplicativos da Kaspersky Lab. A Base de Dados de Conhecimento contém artigos de referência agrupados por tópico.

Na página do aplicativo na Base de Dados de Conhecimento (http://support.kaspersky.com/kis2013), é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos podem responder perguntas que estão fora do escopo do Kaspersky Internet Security, relacionadas a outros aplicativos da Kaspersky Lab. Eles também podem conter notícias do Serviço de Suporte Técnico.

Ajuda online

A ajuda online do aplicativo compreende os arquivos de ajuda.

A ajuda contextual fornece informações sobre cada janela do aplicativo, listando e descrevendo as configurações correspondentes e uma lista de tarefas.

A Ajuda completa fornece informações detalhadas sobre o gerenciamento da proteção do computador, a configuração do aplicativo e a solução de tarefas comuns do usuário.

Documentação

O Manual do Usuário do aplicativo fornece informações sobre como instalar, ativar e configurar o aplicativo, além de dados de operação do aplicativo. O documento também descreve a interface do aplicativo e fornece maneiras de resolver as tarefas normais do usuário ao trabalhar com o aplicativo.

DISCUTINDO OS APLICATIVOS DA KASPERSKY LAB NO FÓRUM

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários no nosso fórum (http://forum.kaspersky.com).

Neste fórum, é possível exibir os tópicos existentes, deixar seus comentários e criar novos tópicos de discussão.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE VENDAS

Se você tiver dúvidas sobre como selecionar, comprar ou renovar o aplicativo, poderá entrar em contato com os especialistas do nosso Departamento de Vendas de uma das seguintes maneiras:

- Ligando para o nosso escritório central em Moscou por telefone (http://www.kaspersky.com/contacts).
- Enviando uma mensagem com sua pergunta para sales@kaspersky.com.

O serviço é fornecido em russo e em inglês.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE LOCALIZAÇÃO E ESCRITA TÉCNICA POR EMAIL

Para entrar em contato com o Departamento de Localização e Escrita Técnica, envie um email para docfeedback@kaspersky.com. Use "Kaspersky Help Feedback: Kaspersky Internet Security" como assunto da mensagem.

KASPERSKY INTERNET SECURITY

Esta seção descreve os recursos do aplicativo e fornece informações resumidas sobre as funções e os componentes do aplicativo. Você saberá os itens que estão incluídos no kit de distribuição e os serviços que estão disponíveis para usuários registrados do aplicativo. Esta seção fornece informações sobre os requisitos de software e hardware que um computador deve atender para permitir a instalação do aplicativo pelo usuário.

NESTA SEÇÃO

Novidades 11

Kit de distribuição 12

Funções principais e aplicativos 12

Serviços para usuários 14

Requisitos de hardware e software 14

NOVIDADES

O Kaspersky Internet Security oferece os novos recursos a seguir:

- A Banca Segura (na página 44) foi adicionada para garantir um uso seguro de serviços bancários online e de sistemas de pagamento, bem como para facilitar as compras online.
- A Proteção da inserção de dados com o teclado do computador (na página 43) foi adicionada, para proteger os dados particulares inseridos em vários sites.
- Para fornecer proteção contra ataques que exploram as vulnerabilidades do software, o recurso de proteção contra exploração foi adicionado ao componente Inspetor do Sistema.
- A funcionalidade do Teclado Virtual (consulte a seção "Teclado Virtual" na página 40) foi melhorada: agora você pode abri-lo clicando no ícone de início rápido, exibido nos campos de inserção de dados nos sites.
- O procedimento de instalação do aplicativo foi simplificado (consulte a seção "Instalando e removendo o aplicativo" na página15).
- O tamanho dos bancos de dados do aplicativo foi reduzido, o que permite diminuir o tamanho dos dados para baixar e acelerar a instalação de atualizações.
- A análise heurística realizada ao verificar sites quanto à presença de phishing foi melhorada.
- A funcionalidade do Antispam foi melhorada, o que fornece uma filtragem mais confiável de email indesejado.
- A funcionalidade do Controle para Pais foi melhorada: foi adicionada a opção para atualizar as regras da verificação de sites por categorias durante a atualização dos bancos de dados. Isso permite um controle mais rigoroso do acesso de crianças a sites com conteúdo explícito.

KIT DE DISTRIBUIÇÃO

Você pode comprar o aplicativo das seguintes maneiras:

- **Na caixa**. Distribuído nas lojas de nossos parceiros.
- **Na Loja Virtual**. Distribuído em lojas virtuais da Kaspersky Lab (por exemplo, http://www.kaspersky.com, seção **Loja Virtual**) ou de empresas parceiras.

Se você comprou a versão do aplicativo na caixa, o kit de distribuição conterá os seguintes itens:

- envelope lacrado com o CD de instalação, que contém os arquivos do aplicativo e da documentação;
- Manual do Usuário resumido com um código de ativação;
- contrato de licença que estipula os termos sob os quais você pode usar o aplicativo.

O conteúdo do kit de distribuição pode ser diferente de acordo com a região na qual o aplicativo é distribuído.

Se você comprar o Kaspersky Internet Security em uma loja virtual, deverá copiar o aplicativo do site da loja. As informações necessárias para a ativação do aplicativo serão enviadas por email após o pagamento.

Para obter mais detalhes sobre as formas de compra e o kit de distribuição, entre em contato com o Departamento de Vendas, enviando uma mensagem para sales@kaspersky.com.

PRINCIPAIS RECURSOS DO APLICATIVO

O Kaspersky Internet Security fornece proteção abrangente ao computador contra ameaças conhecidas e novas, ataques de rede e phishing, spam e outro conteúdo indesejado. Estão disponíveis diferentes funções e componentes de proteção como parte do Kaspersky Internet Security para assegurar proteção completa.

Proteção do Computador

Os componentes de proteção foram concebidos para proteger o computador contra ameaças conhecidas e ameaças novas, ataques de rede, fraude, spam e outras informações indesejadas. Todos os tipos de ameaça são processados por um componente de proteção individual (consulte a descrição de componentes nesta seção). Os componentes podem ser ativados ou desativados de forma independente entre si, e suas configurações podem ser configuradas.

Além da proteção constante assegurada pelos componentes de segurança, é recomendável *verificar* o seu computador regularmente quanto à presença de vírus. Isto é necessário para descartar a possibilidade de disseminação de programas maliciosos que não foram detectados pelos componentes de proteção, por exemplo, devido à definição de um baixo nível de segurança ou por outros motivos.

Para manter o Kaspersky Internet Security atualizado, é necessário *atualizar* os bancos de dados e os módulos de software usados pelo aplicativo.

Algumas tarefas específicas que devem ser executadas ocasionalmente (como a remoção de rastros de atividades de um usuário no sistema), são executadas com *ferramentas avançadas e assistentes*.

Os componentes de proteção que se seguem asseguram proteção em tempo real ao seu computador:

Está descrita abaixo a lógica de funcionamento dos componentes de proteção no modo do Kaspersky Internet Security recomendado pelos peritos da Kaspersky Lab (ou seja, com configurações de aplicativos padrão).

Antivírus de Arquivos

O Antivírus de Arquivos evita a infecção do sistema de arquivos do computador. O componente é inicializado ao iniciar o sistema operacional e permanece continuamente na RAM do computador, verificando todos os arquivos que são abertos, salvos ou iniciados no computador e em todas as unidades conectadas. O Kaspersky Internet Security intercepta todas as tentativas de acessar um arquivo e verifica o arquivo quanto à presença de vírus conhecidos. O arquivo apenas pode ser processado se o arquivo não estiver infetado ou se for tratado com êxito pelo aplicativo. Se não for possível desinfetar um arquivo, por qualquer motivo, ele será excluído. Uma cópia do arquivo será colocada na Quarentena.

Antivírus de Email

O Antivírus de Email verifica as mensagens de email recebidas e enviadas no computador. O email é disponibilizado ao destinatário somente se não contiver objetos perigosos.

Antivírus da Web

O Antivírus da Web intercepta e bloqueia a execução de scripts em sites, caso estes representem uma ameaça. O Antivírus da Web monitora também todo o tráfego da Web e bloqueia o acesso a sites perigosos.

Antivírus de IM

O Antivírus de IM assegura a utilização segura dos pagers da Internet. O componente protege informações que chegam ao computador através de protocolos de IM. O Antivírus de IM assegura o funcionamento seguro de vários aplicativos para envio de mensagens instantâneas.

Controle de Aplicativos

O Controle de Aplicativos registra as ações realizadas pelos aplicativos no sistema e gerencia as atividades dos aplicativos com base no grupo que o componente lhes atribui. É especificado um conjunto de regras para cada grupo de aplicativos. Estas regras gerenciam o acesso de aplicativos a vários recursos do sistema operacional.

Firewall

O Firewall garante a segurança de seu trabalho em redes locais e na Internet. O componente filtra todas as atividades de rede usando regras de dois tipos: *regras para aplicativos* e *regras para pacotes*.

Monitor de Rede

O Monitor de Rede foi concebido para monitorar a atividade na rede em tempo real.

Bloqueador de Ataques de Rede

O Bloqueador de Ataques de Rede é carregado ao inicializar o sistema operacional e rastreia o tráfego de rede recebido quanto à presença de atividades características de ataques de rede. Ao detectar uma tentativa de ataque ao computador, o Kaspersky Internet Security bloqueia toda a atividade de rede do computador que está atacando o seu.

Antispam

O Antispam é integrado no cliente de correio instalado no computador e verifica todas as mensagens de email recebidas quanto à presença de spam. Todas as mensagens que contêm spam são assinaladas com um cabeçalho especial. Você pode configurar o Antispam para processar mensagens de spam de uma forma específica (por exemplo, excluí-las automaticamente ou movê-las para uma pasta especial).

Antiphishing

O Antiphishing permite a verificação de URLs para verificar se estão incluídos na lista de URLs de phishing. Este componente é integrado no Antivírus da Web, Antispam e Antivírus de IM.

Antibanner

O Antibanner bloqueia banners de anúncios em sites e interfaces de aplicativos.

Banca Segura

A Banca Segura fornece proteção dos dados confidenciais ao usar serviços bancários online e sistemas de pagamento, e impede o roubo de ativos ao efetuar pagamentos online.

Controle para Pais

O Controle para Pais foi concebido para proteger crianças e adolescentes contra ameaças relacionadas com o uso do computador e da Internet.

O Controle para Pais permite configurar restrições flexíveis para acessar recursos da Web e aplicativos para diferentes usuários, consoante a respetiva idade. O Controle para Pais permite também exibir relatórios de estatísticas sobre as atividades realizadas pelos usuários controlados.

SERVIÇOS PARA USUÁRIOS

Ao comprar uma licença para o aplicativo, pode beneficiar-se dos seguintes serviços durante todo o termo de validade da licença:

- As atualizações do bancos de dados e o acesso a novas versões do aplicativo
- Consultoria por telefone e por email sobre problemas relacionados à instalação, configuração e uso do aplicativo
- Notificações sobre o lançamento de novos aplicativos da Kaspersky Lab e novos vírus e surtos de vírus. Para usar este serviço, subscreva a newsletter da Kaspersky Lab no site do Serviço de Suporte Técnico.

Não são fornecidas consultorias sobre problemas relacionados ao funcionamento de sistemas operacionais, software e tecnologias de terceiros.

REQUISITOS DE HARDWARE E SOFTWARE

Para assegurar o funcionamento do Kaspersky Internet Security, o computador deve atender aos seguintes requisitos:

Requisitos gerais:

- 480 MB de espaço disponível no disco rígido (incluindo 380 MB na unidade do sistema).
- Unidade de CD/DVD (para instalar o Kaspersky Internet Security do CD de distribuição).
- Acesso à Internet (para a ativação do aplicativo e a atualização dos bancos de dados e módulos do software).
- Microsoft® Internet Explorer® 6.0 ou mais recente
- Microsoft Windows® Installer 2.0.

Requisitos para Microsoft Windows XP Home Edition (Service Pack 2 ou superior), Microsoft Windows XP Professional (Service Pack 2 ou superior) e Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou superior):

- Processador Intel® Pentium® 800 MHz 32 bits (x86)/64 bits (x64) ou superior (ou um equivalente compatível).
- 512 MB de RAM livre.

Requisitos para Microsoft Windows Vista® Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional e Microsoft Windows 7 Ultimate:

- Processador Intel Pentium de 1 GHz 32 bits (x86)/64 bits (x64) ou superior (ou um equivalente compatível).
- 1 GB de RAM disponíveis (para sistemas operacionais de 32 bits); 2 GB de RAM disponíveis (para sistemas operacionais de 64 bits).

INSTALANDO E REMOVENDO O APLICATIVO

Esta seção contém instruções passo a passo para instalação e remoção do aplicativo.

NESTA SEÇÃO

Procedimento de instalação padrão 15

Atualizando a versão anterior do Kaspersky Internet Security 18

Cenários de instalação diferentes do padrão 21

Removendo o aplicativo 21

PROCEDIMENTO DE INSTALAÇÃO PADRÃO

O Kaspersky Internet Security será instalado no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper a atividade do Assistente em qualquer etapa da instalação, feche a janela do Assistente.

Se desejar que o aplicativo proteja mais do que um computador, (com o número máximo de computadores dependendo de sua licença), ele deve ser instalado de forma idêntica em todos os computadores.

- *Para instalar o Kaspersky Internet Security no computador,*

  execute o arquivo de instalação (um arquivo com a extensão EXE) a partir do CD do produto.

Para instalar o Kaspersky Internet Security, você pode também usar um pacote de distribuição baixado da Internet. O Assistente de Configuração exibe algumas etapas de instalação adicionais para alguns idiomas de localização.

NESTA SEÇÃO

Etapa 1. Pesquisar uma versão mais recente do aplicativo 16

Etapa 2. Iniciando a instalação do aplicativo 16

Etapa 3. Examinando o contrato de licença 16

Etapa 4. Declaração sobre coleta de dados do Kaspersky Security Network 16

Etapa 5. Instalação 17

Etapa 6. Concluir a instalação 17

Etapa 7. Ativando o aplicativo 17

Etapa 8. Registrando um usuário 18

Etapa 9. Concluindo a ativação 18

ETAPA 1. PESQUISAR UMA VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o Assistente de Instalação verifica nos servidores de atualização da Kaspersky Lab uma versão mais nova do Kaspersky Internet Security.

Se o Assistente de Configuração não detectar uma nova versão do aplicativo nos servidores de atualização, inicia a instalação da versão atual.

Se o Assistente detectar uma nova versão do Kaspersky Internet Security nos servidores de atualização, solicita o download e a instalação do aplicativo no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem mais aprimoramentos que garantem uma proteção mais confiável do computador. Se recusar instalar a nova versão, o Assistente inicia a instalação da versão atual do aplicativo. Se aceitar instalar a nova versão do aplicativo, o Assistente de Configuração copia os arquivos de configuração do pacote de distribuição para o computador e inicia a instalação da nova versão. Para obter detalhes adicionais sobre como instalar a nova versão do aplicativo, consulte os documentos relevantes.

ETAPA 2. INICIANDO A INSTALAÇÃO DO APLICATIVO

Nesta etapa, o Assistente de Configuração solicita que instale o aplicativo.

Para continuar a instalação, clique no botão **Instalar**.

Consoante o tipo de instalação e o idioma da localização, nesta etapa o Assistente solicita a exibição do Contrato de Licença concluído entre você e a Kaspersky Lab, oferecendo também a possibilidade de participar da Kaspersky Security Network.

ETAPA 3. EXAMINANDO O CONTRATO DE LICENÇA

Esta etapa do Assistente de Configuração é exibida para alguns idiomas de localização, ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição baixado da Internet.

Nesta etapa, o Assistente de Configuração solicita a revisão do Contrato de Licença concluído entre você e a Kaspersky Lab.

Leia cuidadosamente o Contrato de Licença e, se aceitar os termos, clique no botão **Aceitar**. A instalação continuará.

Se não aceitar o Contrato de Licença, o aplicativo não é instalado.

ETAPA 4. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Esta etapa do Assistente de Configuração é exibida para alguns idiomas de localização, ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição baixado da Internet.

Nesta etapa, você será convidado pelo Assistente de Configuração a participar da Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os aplicativos assinados baixados no seu computador, além das informações do seu sistema. Nenhum dado particular recebido é coletado, processado ou armazenado.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Se você concordar com todos os termos da Declaração, selecione a caixa **Desejo participar do programa Kaspersky Security Network** na janela do Assistente.

Clique no botão **Avançar** para continuar com a instalação do Assistente.

ETAPA 5. INSTALAÇÃO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

O Kaspersky Internet Security realiza várias verificações durante a instalação. Estas verificações podem resultar na detecção dos seguintes problemas:

- **Não conformidade do sistema operacional com os requisitos de software**. Durante a instalação, o Assistente verifica as seguintes condições:

  - Se o sistema operacional e os Service Packs atendem aos requisitos de software
  - Se todos os aplicativos necessários estão disponíveis
  - Se a quantidade de espaço livre em disco é suficiente para a instalação.

  Se algum dos requisitos acima não for atendido, será exibida uma notificação correspondente na tela.

- **Presença de aplicativos incompatíveis no computador**. Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e será solicitado que você os remova. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Internet Security deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Internet Security continuará automaticamente.

- **Presença de software malicioso no computador**. Se forem detectados aplicativos maliciosos no computador que interferem com a instalação de software antivírus, o Assistente de Configuração solicita o download de uma ferramenta dedicada concebida para neutralizar a infecção, com o nome *Ferramenta de Remoção de Vírus Kaspersky*.

  Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

ETAPA 6. CONCLUIR A INSTALAÇÃO

Nesta etapa, o Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo. Para executar o Kaspersky Internet Security de imediato, confirme se a caixa **Executar o Kaspersky Internet Security 2013** está selecionada e clique no botão **Concluir**.

Em alguns casos, pode ser necessário reiniciar o sistema operacional para concluir a instalação. Se a caixa **Executar o Kaspersky Internet Security 2013** estiver selecionada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa **Executar o Kaspersky Internet Security 2013** antes de fechar o Assistente, é necessário executar o aplicativo manualmente.

ETAPA 7. ATIVANDO O APLICATIVO

Nesta etapa, o Assistente de Configuração solicita que ative o aplicativo.

Ativação é o processo de pôr em operação uma versão totalmente funcional do aplicativo por um determinado período de tempo.

Caso tenha comprado uma licença para o Kaspersky Internet Security e tenha baixado o aplicativo a partir da loja virtual, a ativação do aplicativo pode ser realizada durante a instalação.

As seguintes opções de ativação do Kaspersky Internet Security estarão disponíveis:

- **Ativar a versão comercial**. Selecione essa opção e insira o código de ativação (consulte seção "Sobre o código de ativação" na página 24) caso tenha comprado uma versão comercial do aplicativo.

  Se você especificar um código de ativação do Kaspersky Anti-Virus no campo de entrada, o procedimento para migrar para o Kaspersky Anti-Virus será iniciado após a conclusão da ativação.

- **Ativar a versão de avaliação**. Use esta opção de ativação se desejar instalar a versão de avaliação do aplicativo antes de decidir comprar a versão comercial. Você poderá usar a versão totalmente funcional do aplicativo durante o período limitado pela licença de avaliação. Quando a licença expirar, a versão de avaliação não poderá ser ativada pela segunda vez.

Você precisará de uma conexão com a Internet para ativar o aplicativo.

ETAPA 8. REGISTRANDO UM USUÁRIO

Esta etapa está disponível somente ao ativar a versão comercial do aplicativo. Na ativação da versão de avaliação, essa etapa é ignorada.

Os usuários registrados podem enviar pedidos para o Serviço de Suporte Técnico e para o Laboratório de Vírus através da Minha conta Kaspersky no site da Kaspersky Lab, gerenciar códigos de ativação com maior conveniência e receber as informações mais recentes sobre novos produtos e ofertas especiais.

Se você concordar em se registrar, especifique a data do registro nos campos correspondentes e clique no botão **Avançar** para enviar os dados para a Kaspersky Lab.

Em alguns casos, é necessário o registro do usuário para iniciar o uso do aplicativo.

ETAPA 9. CONCLUINDO A ATIVAÇÃO

O Assistente informará que o Kaspersky Internet Security foi ativado com êxito. Além disso, são fornecidas informações sobre a licença atual nesta janela: o tipo de licença (comercial ou de avaliação), a data de expiração e o número de hosts abrangidos pela licença.

Se você tiver solicitado uma assinatura, serão exibidas informações sobre o status da assinatura em vez da data de expiração da licença.

Clique no botão **Concluir** para fechar o assistente.

ATUALIZANDO A VERSÃO ANTERIOR DO KASPERSKY INTERNET SECURITY

Se o Kaspersky Internet Security 2011 ou 2012 já estiver instalado no computador, atualize o aplicativo para o Kaspersky Internet Security 2013. Se você tiver uma licença atualizada do Kaspersky Anti-Virus 2011 ou 2012, não será necessário ativar o aplicativo: o Assistente de Instalação recuperará as informações da licença do Kaspersky Internet Security 2011 ou 2012 automaticamente e as aplicará durante o processo de instalação.

O Kaspersky Internet Security será instalado no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper a atividade do Assistente em qualquer etapa da instalação, feche a janela do Assistente.

Se desejar que o aplicativo proteja mais do que um computador, (com o número máximo de computadores dependendo de sua licença), ele deve ser instalado de forma idêntica em todos os computadores.

- *Para instalar o Kaspersky Internet Security no computador,*

  execute o arquivo de instalação (um arquivo com a extensão EXE) a partir do CD do produto.

  Para instalar o Kaspersky Internet Security, você pode também usar um pacote de distribuição baixado da Internet. O Assistente de Configuração exibe algumas etapas de instalação adicionais para alguns idiomas de localização.

NESTA SEÇÃO

Etapa 1. Pesquisar uma versão mais recente do aplicativo 19

Etapa 2. Iniciando a instalação do aplicativo 19

Etapa 3. Examinando o contrato de licença 20

Etapa 4. Declaração sobre coleta de dados do Kaspersky Security Network 20

Etapa 5. Instalação 20

Etapa 6. Concluir a instalação 21

ETAPA 1. PESQUISAR UMA VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o Assistente de Instalação verifica nos servidores de atualização da Kaspersky Lab uma versão mais nova do Kaspersky Internet Security.

Se o Assistente de Configuração não detectar uma nova versão do aplicativo nos servidores de atualização, inicia a instalação da versão atual.

Se o Assistente detectar uma nova versão do Kaspersky Internet Security nos servidores de atualização, solicita o download e a instalação do aplicativo no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem mais aprimoramentos que garantem uma proteção mais confiável do computador. Se recusar instalar a nova versão, o Assistente inicia a instalação da versão atual do aplicativo. Se aceitar instalar a nova versão do aplicativo, o Assistente de Configuração copia os arquivos de configuração do pacote de distribuição para o computador e inicia a instalação da nova versão. Para obter detalhes adicionais sobre como instalar a nova versão do aplicativo, consulte os documentos relevantes.

ETAPA 2. INICIANDO A INSTALAÇÃO DO APLICATIVO

Nesta etapa, o Assistente de Configuração solicita que instale o aplicativo.

Para continuar a instalação, clique no botão **Instalar**.

Consoante o tipo de instalação e o idioma da localização, nesta etapa o Assistente solicita a exibição do Contrato de Licença concluído entre você e a Kaspersky Lab, oferecendo também a possibilidade de participar da Kaspersky Security Network.

ETAPA 3. EXAMINANDO O CONTRATO DE LICENÇA

Esta etapa do Assistente de Configuração é exibida para alguns idiomas de localização, ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição baixado da Internet.

Nesta etapa, o Assistente de Configuração solicita a revisão do Contrato de Licença concluído entre você e a Kaspersky Lab.

Leia cuidadosamente o Contrato de Licença e, se aceitar os termos, clique no botão **Aceitar**. A instalação continuará.

Se não aceitar o Contrato de Licença, o aplicativo não é instalado.

ETAPA 4. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Esta etapa do Assistente de Configuração é exibida para alguns idiomas de localização, ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição baixado da Internet.

Nesta etapa, você será convidado pelo Assistente de Configuração a participar da Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os aplicativos assinados baixados no seu computador, além das informações do seu sistema. Nenhum dado particular recebido é coletado, processado ou armazenado.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Se você concordar com todos os termos da Declaração, selecione a caixa **Desejo participar do programa Kaspersky Security Network** na janela do Assistente.

Clique no botão **Avançar** para continuar com a instalação do Assistente.

ETAPA 5. INSTALAÇÃO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

O Kaspersky Internet Security realiza várias verificações durante a instalação. Estas verificações podem resultar na detecção dos seguintes problemas:

- **Não conformidade do sistema operacional com os requisitos de software**. Durante a instalação, o Assistente verifica as seguintes condições:
  - Se o sistema operacional e os Service Packs atendem aos requisitos de software
  - Se todos os aplicativos necessários estão disponíveis
  - Se a quantidade de espaço livre em disco é suficiente para a instalação.

  Se algum dos requisitos acima não for atendido, será exibida uma notificação correspondente na tela.
- **Presença de aplicativos incompatíveis no computador**. Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e será solicitado que você os remova. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Internet Security deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Internet Security continuará automaticamente.

- **Presença de software malicioso no computador**. Se forem detectados aplicativos maliciosos no computador que interferem com a instalação de software antivírus, o Assistente de Configuração solicita o download de uma ferramenta dedicada concebida para neutralizar a infecção, com o nome *Ferramenta de Remoção de Vírus Kaspersky*.

  Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

ETAPA 6. CONCLUIR A INSTALAÇÃO

Esta janela do Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo.

Reinicie o sistema operacional depois da instalação do aplicativo.

Se a caixa **Executar o Kaspersky Internet Security** estiver marcada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa **Executar o Kaspersky Internet Security** antes de fechar o Assistente, é necessário executar o aplicativo manualmente.

CENÁRIOS DE INSTALAÇÃO DIFERENTES DO PADRÃO

Esta seção descreve cenários de instalação do aplicativo diferentes da instalação padrão ou da atualização da versão anterior.

Instalando o Kaspersky Internet Security e ativando o aplicativo usando um código de ativação para o Kaspersky Anti-Virus

Se, ao instalar o Kaspersky Internet Security, na etapa Ativando o aplicativo, você inserir um código de ativação do Kaspersky Anti-Virus, o Assistente de Migração será iniciado, resultando na instalação do Kaspersky Anti-Virus no computador.

Se, ao instalar o Kaspersky Internet Security, na etapa Ativando o aplicativo, você selecionar **Ativar mais tarde** e ativar o aplicativo instalado usando um código de ativação do Kaspersky Anti-Virus, o Assistente de Migração será também iniciado, resultando na instalação do Kaspersky Anti-Virus no computador.

Instalando o Kaspersky Internet Security 2013 sobre o Kaspersky Anti-Virus 2011 ou 2012

Se você executar a instalação do Kaspersky Internet Security 2013 em um computador em que o Kaspersky Anti-Virus 2011 ou 2012 com uma licença ativa já estiver instalado, o Assistente de Instalação detectará isso e solicitará que você selecione um dos seguintes cenários:

- Continuar a utilização do Kaspersky Anti-Virus com a licença atual. Nesse caso, o Assistente de Migração será iniciado, resultando na instalação do Kaspersky Anti-Virus 2013 no computador. Você poderá usar o Kaspersky Anti-Virus 2013 enquanto a licença do Kaspersky Anti-Virus 2011 ou 2012 for efetiva.

- Continuar a instalação do Kaspersky Internet Security 2013. Nesse caso, o procedimento de instalação continuará de acordo com o cenário padrão a partir da etapa Ativando o aplicativo.

REMOVENDO O APLICATIVO

Depois que o Kaspersky Internet Security for desinstalado, o computador e seus dados pessoais estarão desprotegidos.

O Kaspersky Internet Security será desinstalado com a ajuda do Assistente de Instalação.

Para iniciar o Assistente,

no menu **Iniciar**, selecione **Programas → Kaspersky Internet Security 2013 → Remover o Kaspersky Internet Security 2013**.

NESTA SEÇÃO

Etapa 1. Salvar dados para uso futuro 22

Etapa 2. Confirmando a remoção do aplicativo 22

Etapa 3. Removendo o aplicativo. Concluindo a remoção 22

ETAPA 1. SALVAR DADOS PARA USO FUTURO

Nesta etapa, é possível especificar os dados usados pelo aplicativo que você deseja manter para reutilizar na próxima instalação do aplicativo (por exemplo, ao instalar uma versão mais nova do aplicativo).

Por padrão, o aplicativo solicita que salve as informações sobre a ativação.

Para salvar dados do aplicativo para uso futuro:

1. Selecione as caixas de seleção junto dos tipos de dados que deseja salvar:

   - **Informações da Licença** – um conjunto de dados que elimina a necessidade de ativar o novo aplicativo através da permissão de uso sob a licença atual, a menos que a licença expire antes do início da instalação.
   - **Arquivos da Quarentena** – arquivos verificados pelo aplicativo e movidos para a Quarentena.

     Após o Kaspersky Internet Security ser removido do computador, os arquivos da Quarentena ficam indisponíveis. Você deve instalar o Kaspersky Internet Security para processar esses arquivos.

   - **Configurações de funcionamento do aplicativo** são os valores das configurações do aplicativo selecionadas durante a configuração.
   - **Dados do iChecker** são arquivos que contêm informações sobre os objetos que já foram verificados pela tecnologia iChecker.
   - **Bancos de dados do Antispam** são bancos de dados que contêm assinaturas de mensagens de spam baixadas e gravadas pelo aplicativo.

ETAPA 2. CONFIRMANDO A REMOÇÃO DO APLICATIVO

Como a remoção do aplicativo ameaça a segurança do computador e de seus dados pessoais, será solicitado que você confirme sua intenção de remover o aplicativo. Para fazer isso, clique no botão **Remover**.

ETAPA 3. REMOVENDO O APLICATIVO. CONCLUINDO A REMOÇÃO

Nesta etapa, o Assistente remove o aplicativo do computador. Aguarde a conclusão da remoção.

Ao remover o aplicativo, você deve reiniciar o sistema operacional. Se você cancelar a reinicialização imediata, a conclusão do procedimento de remoção será adiada até que o sistema operacional seja reiniciado ou o computador seja desligado e reiniciado.

LICENÇA DO APLICATIVO

Esta seção fornece informações sobre os termos gerais relacionados à ativação do aplicativo. Leia esta seção para saber mais sobre a finalidade do contrato de licença, os tipos de licença, as formas de ativação do aplicativo e a renovação da licença.

NESTA SEÇÃO

Sobre o Contrato de Licença do Usuário Final 23

Sobre a licença 23

Sobre o código de ativação 24

Sobre o fornecimento de dados 24

SOBRE O CONTRATO DE LICENÇA DO USUÁRIO FINAL

O Contrato de Licença do Usuário Final é um contrato vinculativo entre o usuário e a Kaspersky Lab ZAO, que estipula os termos em que poderá usar o aplicativo.

Leia atentamente todos os termos do Contrato de Licença antes de começar a usar o aplicativo.

É considerado que os termos do Contrato de Licença foram aceites, confirmando que você concorda com o Acordo de Licença ao instalar o aplicativo. Se você não aceitar os termos do Contrato de Licença, você deve abortar a instalação do aplicativo ou renunciar ao uso do aplicativo.

SOBRE A LICENÇA

Uma *licença* é um direito limitado no tempo para usar o aplicativo, concedido ao abrigo do Contrato de Licença de Usuário Final. A licença estipula um código exclusivo para a ativação da sua cópia do Kaspersky Internet Security.

Uma licença atual dá-lhe o direito de usar os seguintes tipos de serviços:

- O direito de usar o aplicativo em um ou vários dispositivos.

  O número de dispositivos nos quais você pode usar o aplicativo está especificado no Contrato de Licença.

- Assistência do Suporte Técnico da Kaspersky Lab.

- Outros serviços disponíveis a partir da Kaspersky Lab ou respetivos parceiros durante o termo da licença (consulte a seção "Serviço para usuários" na página 14).

O escopo dos serviços e o termo de uso do aplicativo dependem do tipo de licença pela qual o aplicativo foi ativado.

São oferecidos os seguintes tipos de licença:

- *Avaliação* – uma licença gratuita que permite testar o aplicativo.

  A licença de avaliação geralmente tem um termo curto. Assim que a licença expirar, todos os recursos do Kaspersky Internet Security serão desativados. Para continuar usando o aplicativo, você deverá comprar uma licença comercial.

- *Comercial* – uma licença paga, oferecida ao comprar o aplicativo.

  Quando a licença comercial expira, o aplicativo continua a ser executado, mas apresenta uma funcionalidade limitada (por exemplo, a atualização e o uso do Kaspersky Security Network não ficam disponíveis). Você poderá continuar a beneficiar de todos os componentes do aplicativo e a realizar verificações de vírus e outro software malicioso, mas usando apenas os bancos de dados instalados no computador antes da licença expirar. Para continuar a usar o Kaspersky Internet Security no modo totalmente funcional, você deve renovar sua licença comercial.

  É recomendável renovar a licença antes da expiração, para assegurar proteção máxima do computador contra todas as ameaças de segurança.

SOBRE O CÓDIGO DE ATIVAÇÃO

O *código de ativação* é um código que você recebe ao comprar a licença comercial do Kaspersky Internet Security. Esse código é necessário para a ativação do aplicativo.

O código de ativação é uma sequência exclusiva de vinte dígitos e caracteres latinos no formato xxxxx-xxxxx-xxxxx-xxxxx.

Dependendo da forma como comprou o aplicativo, poderá obter o código de ativação através de uma das seguintes formas:

- Se você comprou a versão na caixa do Kaspersky Internet Security, o código de ativação será especificado na documentação ou na caixa que contém o CD de instalação.

- Se você comprou o Kaspersky Internet Security em uma loja virtual, o código de ativação será enviado para o email especificado ao solicitar o produto.

A contagem do termo de licença começa a partir da data em que ativou o aplicativo. Se você tiver comprado uma licença destinada ao uso do Kaspersky Internet Security em vários dispositivos, o termo da licença começará no momento em que você aplicar o código de ativação pela primeira vez.

Se você perder ou excluir acidentalmente seu código após a ativação, deverá enviar uma solicitação ao Serviço de Suporte Técnico da Kaspersky Lab através da Minha conta Kaspersky (consulte a seção "Obtendo suporte técnico através da Minha conta Kaspersky" na página 63).

SOBRE O FORNECIMENTO DE DADOS

Para aumentar o nível de proteção, aceitando os termos do Contrato de Licença, você aceita fornecer as seguintes informações à Kaspersky Lab no modo automático:

- informações sobre somas de verificação de objetos processados (MD5);

- informações necessárias para acessar as reputações de URLs;

- estatísticas sobre o uso de notificações de produtos;

- dados estatísticos para proteção contra spam;

- dados sobre a ativação do Kaspersky Internet Security e a versão atualmente sendo usada;
- informações sobre os tipos de ameaças detectadas;
- informações sobre certificados digitais atualmente em uso e informações necessárias para os verificar.

Se o computador estiver equipado com TPM (Trusted Platform Module), você aceita também fornecer à Kaspersky Lab o relatório de TPM sobre a inicialização do sistema operacional e as informações necessárias para o verificar. Caso ocorra um erro durante a instalação do Kaspersky Internet Security, você aceita fornecer à Kaspersky Lab informações sobre o código de erro, o pacote de distribuição sendo usado e o computador, em modo automático.

Em caso de participação da Kaspersky Security Network (consulte a seção "Participando da Kaspersky Security Network (KSN)" na página 60), as seguintes informações serão automaticamente enviadas do computador para a Kaspersky Lab:

- informações sobre o hardware e software instalados no computador;
- informações sobre o status da proteção antivírus do computador, bem como todos os objetos e ações potencialmente maliciosos e as decisões tomadas em relação a esses objetos e ações;
- informações sobre os aplicativos sendo baixados e executados;
- informações sobre erros da interface e o uso da interface do Kaspersky Internet Security;
- informações sobre a versão dos bancos de dados atualmente sendo usados;
- estatísticas de atualizações e conexões aos servidores da Kaspersky Lab.

Além disso, a verificação adicional da Kaspersky Lab pode requerer o envio de arquivos (ou partes de arquivos) expostos a um elevado risco de exploração por invasores, com o objetivo de danificar o computador ou os dados do usuário.

As informações transferidas não contêm dados particulares e outros tipos de informações confidenciais. As informações recuperadas são protegidas pela Kaspersky Lab de acordo com os requisitos estipulados pela legislação existente. Para mais detalhes sobre o fornecimento de dados, consulte o site (http://support.kaspersky.com).

SOLUCIONANDO TAREFAS TÍPICAS

Esta seção contém instruções passo a passo para executar tarefas de usuário comuns que podem ser realizadas no aplicativo.

NESTA SEÇÃO

Ativando o aplicativo 27

Comprando e renovando uma licença 28

Gerenciando notificações do aplicativo 28

Avaliando o status de proteção do computador e solucionando problemas de segurança 29

Atualizando bancos de dados e módulos do aplicativo 30

Verificar as áreas críticas do computador quanto à presença de vírus 30

Verificação completa do computador quanto à presença de vírus 30

Verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus 31

Verificando objetos provavelmente infetados 32

Restaurando um arquivo excluído ou desinfetado pelo aplicativo 32

Recuperando o sistema operacional após infecção 33

Verificando email e filtrando anexos em mensagens de email 35

Bloqueando email indesejado (spam) 36

Verificar o computador quanto à presença de vulnerabilidades 36

Processando aplicativos desconhecidos 36

Protegendo dados particulares contra roubo 39

Avaliando o status de segurança de um site 47

Bloqueando o acesso a sites de várias regiões 47

Aplicando o Controle para Pais a usuários do computador 48

Usando o Perfil de Jogo para modo de tela inteira 50

Criar e usar o Disco de Recuperação 50

Protegendo por senha o acesso ao Kaspersky Internet Security 53

Pausando e reiniciando a proteção do computador 54

Exibindo o relatório de operação do aplicativo 55

Restaurando as configurações padrão do aplicativo 55

Importando as configurações do aplicativo para o Kaspersky Internet Security instalado em outro computador 58

Usando o Kaspersky Gadget 58

A participação na Kaspersky Security Network (KSN) 60

ATIVANDO O APLICATIVO

Você necessita de ativar o aplicativo para poder usar sua funcionalidade e serviços associados.

Se você não ativou o aplicativo durante a instalação, pode fazer isso posteriormente. Você será lembrado da necessidade de ativar o aplicativo por mensagens do Kaspersky Internet Security que serão exibidas na área de notificação da barra de tarefas. O Kaspersky Internet Security pode ser ativado usando o Assistente de Ativação.

Para executar o Assistente de Ativação do Kaspersky Internet Security:

- Clique no link **Ativar** na janela de notificação do Kaspersky Internet Security exibida na área de notificação da barra de tarefas.
- Clique no link **Insira seu código de ativação aqui** na parte inferior da janela principal do aplicativo. Na janela **Licença** que é aberta, clique no botão **Ativar o aplicativo** .

Ao trabalhar com o Assistente de Ativação do Aplicativo, você deve especificar valores para diversas configurações.

Step 1. Inserir o código de ativação

Insira o código de ativação (consulte a seção "Sobre o código de ativação" na página 24) no campo correspondente e clique no botão **Avançar**.

Step 2. Solicitando a ativação

Se a solicitação de ativação for enviada com êxito, o Assistente continuará automaticamente na etapa seguinte.

Step 3. Inserindo dados de registro

Os usuários registrados podem usar os seguintes recursos:

- Enviar solicitações ao Serviço de Suporte Técnico e ao Laboratório de Antivírus a partir da Minha conta Kaspersky no site da Kaspersky Lab.
- Gerenciar códigos de ativação.
- Receber informações sobre novos produtos e ofertas especiais da Kaspersky Lab.

Especifique seus dados de registro e clique no botão **Avançar**.

Step 4. Ativação

Se a ativação do aplicativo tiver êxito, o Assistente continuará automaticamente na etapa seguinte.

Step 5. Conclusão do Assistente

Esta janela do Assistente exibe informações sobre os resultados da ativação.

Clique no botão **Concluir** para fechar o assistente.

COMPRANDO E RENOVANDO UMA LICENÇA

Se você tiver instalado o Kaspersky Internet Security sem uma licença, poderá comprar uma após a instalação. Ao comprar uma licença, você receberá um código de ativação que deve ser aplicado para ativar o aplicativo (consulte a seção "Como ativar o aplicativo" na página 27).

Quando sua licença expirar, você poderá renová-la. Para isso, você pode adicionar um código de ativação de reserva sem ter de esperar que a licença atual expire. Quando a licença atual expirar, o Kaspersky Internet Security será ativado automaticamente através do código de ativação de reserva.

Para comprar uma licença:

1. Abra a janela principal do aplicativo.
2. Clique no link **Insira o código de ativação aqui/Licença** na parte inferior da janela principal para abrir a janela **Licença**.
3. Na janela que é aberta, clique no botão **Comprar código de ativação**.

   A página da loja virtual na Web na qual você pode comprar uma licença é aberta.

Para adicionar um código de ativação de reserva:

1. Abra a janela principal do aplicativo.
2. Clique no link **Insira o código de ativação aqui/Licença** na parte inferior da janela principal para abrir a janela **Licença**.
3. Na janela que é aberta, clique no botão **Inserir código de ativação**.

   O Assistente de Ativação do aplicativo é aberto.
4. Insira o código de ativação nos campos correspondentes e clique no botão **Avançar**.

   Em seguida, o Kaspersky Internet Security envia os dados para serem verificados pelo servidor de ativação. Se a verificação tiver êxito, o Assistente de Ativação continuará automaticamente na etapa seguinte.
5. Ao concluir com o Assistente, clique no botão **Concluir**.

GERENCIANDO NOTIFICAÇÕES DO APLICATIVO

As notificações que são exibidas na área de notificação da barra de tarefas informam sobre eventos ocorridos durante a operação do aplicativo e que exigem sua atenção. Dependendo do grau de importância do evento, você poderá receber os seguintes tipos de notificações:

- *Notificações críticas* – informam sobre os eventos de importância crítica para a segurança do computador, como a detecção de um objeto malicioso ou uma atividade perigosa no sistema. As janelas das notificações e mensagens pop-up críticas são vermelhas.
- *Notificações importantes* – informam sobre os eventos que possivelmente são importantes para a segurança do computador, como a detecção de um objeto provavelmente infetado ou uma atividade suspeita no sistema. As janelas das notificações e mensagens pop-up importantes são amarelas.
- *Notificações informativas* – informam sobre os eventos que não têm importância crítica para a segurança do computador. As janelas das notificações e mensagens pop-up informativas são verdes.

Se for exibida alguma dessas notificações na tela, selecione uma das opções sugeridas. A opção ideal é aquela recomendada como padrão pelos especialistas da Kaspersky Lab.

AVALIANDO O STATUS DE PROTEÇÃO DO COMPUTADOR E SOLUCIONANDO PROBLEMAS DE SEGURANÇA

Os problemas com a proteção do computador são indicados pelo indicador localizado à esquerda da janela principal do aplicativo (consulte a figura, abaixo). O indicador tem a forma de um ícone de monitor que muda de cor de acordo com o status de proteção do computador: o verde significa que o computador está protegido, o amarelo indica problemas relacionados à proteção, o vermelho alerta sobre ameaças graves à segurança do computador. É recomendável corrigir os problemas e as ameaças de segurança imediatamente.

Figura 1. Indicador do status de proteção

Ao clicar no indicador na janela principal do aplicativo, é aberta a janela **Problemas de Segurança** (veja a figura a seguir), que contém informações detalhadas sobre o status de proteção do computador e sugestões para a solução dos problemas e ameaças detectados.

Figura 2. A janela Problemas de Segurança

Os problemas com a proteção são agrupados em categorias. Para cada problema, são listadas ações que podem ser usadas para solucionar o problema.

ATUALIZANDO BANCOS DE DADOS E MÓDULOS DO APLICATIVO

Por padrão, o Kaspersky Internet Security verifica automaticamente as atualizações nos servidores de atualização da Kaspersky Lab. Se o servidor armazenar um conjunto de atualizações recentes, o Kaspersky Internet Security as baixará e instalará em segundo plano. Você pode executar uma atualização do Kaspersky Internet Security manualmente em qualquer altura a partir da janela principal do aplicativo ou a partir do menu de contexto do ícone do aplicativo na área de notificação da barra de tarefas.

Para baixar atualizações dos servidores da Kaspersky Lab, é necessário estar conectado à Internet.

- *Para executar uma atualização no menu de contexto do ícone do aplicativo na área de notificações da barra de tarefas,*

  no menu de contexto do ícone do aplicativo, selecione o item **Atualização**.

- *Para executar uma atualização da janela principal do aplicativo:*

  1. Abra a janela principal do aplicativo e selecione a seção **Atualização** na parte inferior da janela.
  2. Na janela **Atualização** que é aberta, clique no botão **Executar atualização**.

VERIFICAR AS ÁREAS CRÍTICAS DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

A verificação de áreas críticas compreende a verificação dos seguintes objetos:

- objetos carregados ao iniciar o sistema operacional;
- memória do sistema;
- setores de inicialização do disco.

- *Para iniciar a verificação na janela principal do aplicativo:*

  1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
  2. Na janela **Verificação** que é aberta, na seção **Verificação de Áreas Críticas**, clique no botão .

VERIFICAÇÃO COMPLETA DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

Durante uma verificação completa, o Kaspersky Internet Security verifica os seguintes objetos por padrão:

- memória do sistema;
- objetos carregados ao iniciar o sistema operacional;
- backup do sistema;
- discos rígidos e unidades removíveis.

É recomendável realizar uma verificação completa imediatamente depois de instalar o Kaspersky Internet Security no computador.

Para iniciar a verificação completa na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
2. Na janela **Verificação** que é aberta, na seção **Verificação Completa**, clique no botão .

VERIFICAR UM ARQUIVO, PASTA, DISCO OU OUTRO OBJETO QUANTO À PRESENÇA DE VÍRUS

Você pode usar os seguintes métodos para verificar um objeto quanto à presença de vírus:

- no menu de contexto do objeto;
- na janela principal do aplicativo;
- Usando o Gadget do Kaspersky Internet Security (consulte a seção "Usando o Kaspersky Gadget" na página 58) (apenas para sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).

Para iniciar uma verificação de vírus no menu de contexto do objeto:

1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o objeto que deve ser verificado.
2. Clique com o botão direito do mouse no menu de contexto do objeto (veja a figura a seguir) e selecione **Verificar Vírus**.

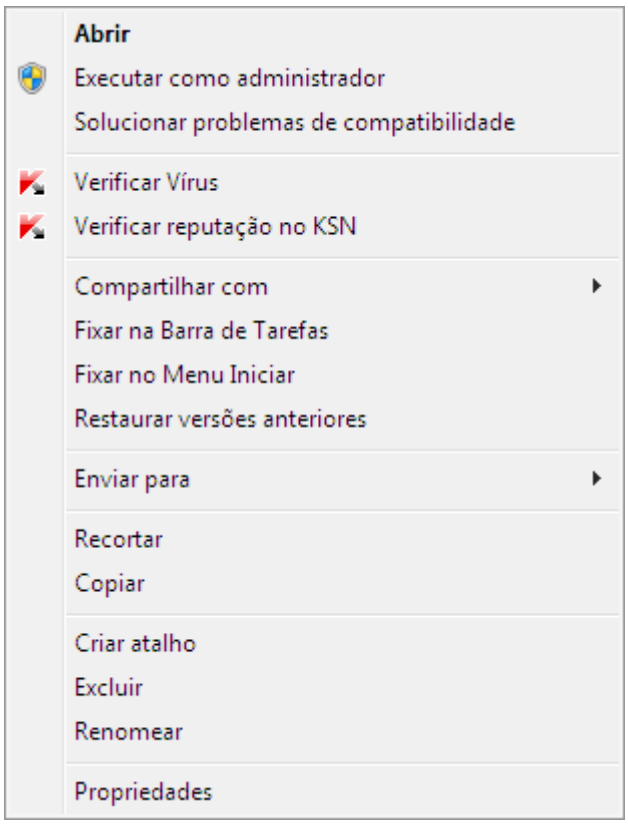

Figura 3. O menu de contexto de um objeto no Microsoft Windows

- *Para iniciar a verificação de um objeto na janela principal do aplicativo:*

  1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
  2. Clique no link **Especificar** na parte inferior da janela, à direita, para abrir a janela **Verificação Personalizada** e marque as caixas ao lado das pastas e unidades que você deseja verificar.

     Se a janela não exibir nenhum objeto a ser verificado:

     a. Clique no botão **Adicionar**.

     b. Na janela **Selecionar objeto a ser verificado** que é aberta, selecione um objeto.

- *Para verificar um objeto quanto à presença de vírus usando o gadget,*

  arraste o objeto a ser verificado para o gadget.

VERIFICANDO OBJETOS PROVAVELMENTE INFETADOS

Se você suspeitar que um objeto está infetado, primeiro verifique-o usando o Kaspersky Internet Security (consulte a seção "Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus" na página 31).

Se o aplicativo concluir a verificação e considerar que um objeto não está infetado, mas você suspeitar do contrário, pode enviar esse objeto para o *Laboratório de Antivírus*: Os especialistas do Laboratório de Vírus verificam o objeto. Se um objeto estiver infetado com um vírus, será adicionado à descrição dos novos vírus nos bancos de dados que serão baixados pelo aplicativo com uma atualização (consulte a seção "Atualizando os bancos de dados e módulos do aplicativo" na página 30).

- *Para enviar um arquivo para o Laboratório de Vírus:*

  1. Vá para a página de solicitação do Laboratório de Vírus (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt).
  2. Siga as instruções na página para enviar sua solicitação.

RESTAURANDO UM ARQUIVO EXCLUÍDO OU DESINFETADO PELO APLICATIVO

A Kaspersky Lab recomenda que você evite restaurar objetos excluídos e desinfetados, pois eles podem representar uma ameaça ao computador.

Para restaurar um objeto excluído ou desinfetado, você pode usar sua cópia de backup criada pelo aplicativo durante uma verificação do objeto.

- *Para restaurar um arquivo excluído ou desinfetado pelo aplicativo:*

  1. Abra a janela principal do aplicativo.
  2. Na parte inferior da janela, selecione a seção **Quarentena**.

3. Na janela **Quarentena** que é exibida, selecione o arquivo desejado na lista e clique no botão **Restaurar** (consulte a imagem abaixo).

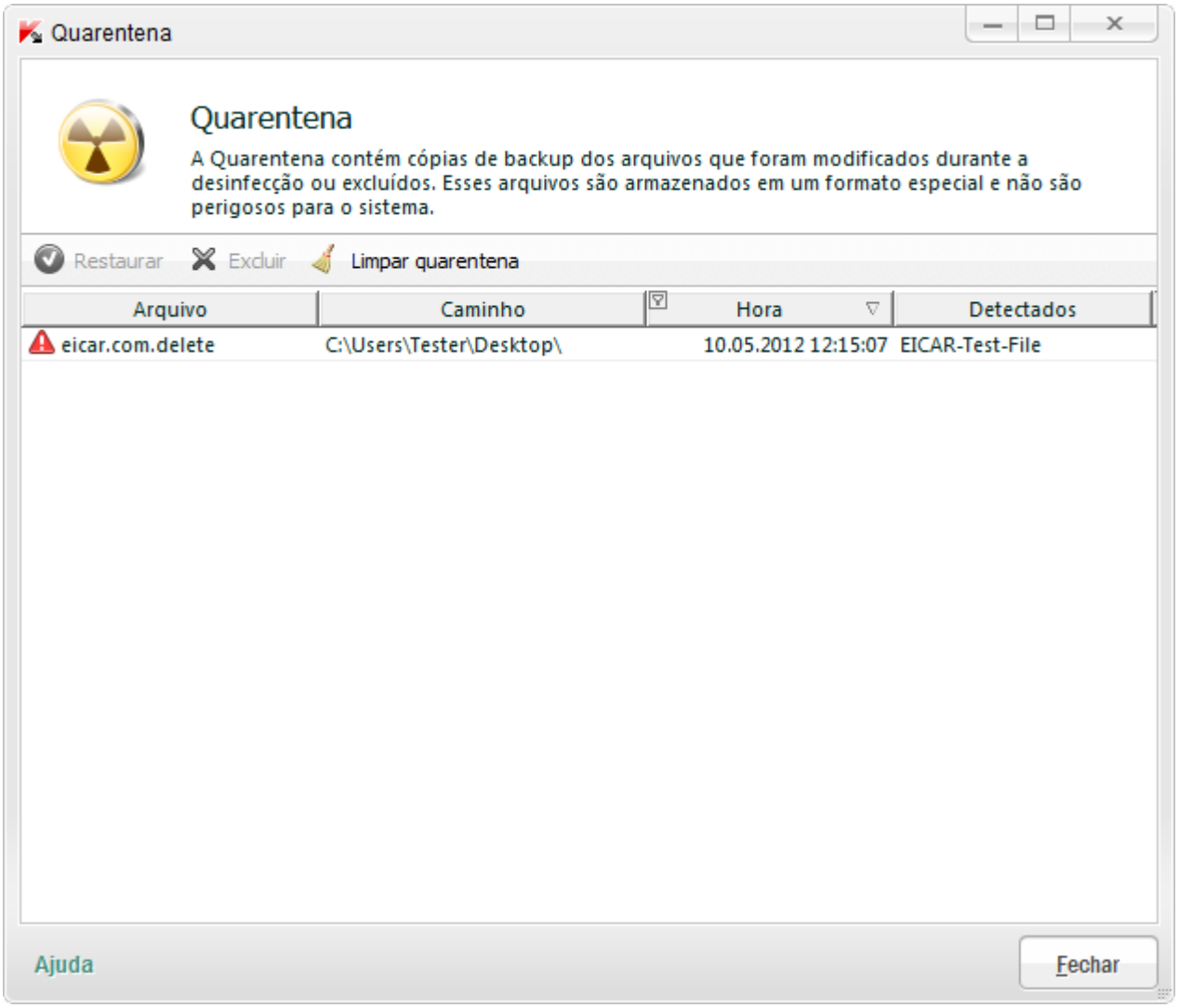

*Figura 4. Janela **Quarentena***

RECUPERANDO O SISTEMA OPERACIONAL APÓS INFECÇÃO

Se você suspeitar que o sistema operacional do computador foi corrompido ou modificado devido a atividade de software malicioso ou uma falha do sistema, use o *assistente de solução de problemas pós-infecção do Microsoft Windows* que limpa o sistema de qualquer rastro de objetos maliciosos. A Kaspersky Lab recomenda executar o Assistente depois de desinfetar o computador para assegurar que todas as ameaças e os danos causados pelas infecções tenham sido corrigidos.

O Assistente verifica se existem alterações ao sistema, como as seguintes: acesso à rede bloqueado, extensões de formato de arquivo conhecido com alterações, bloqueio da barra de ferramentas e outros. Existem diferentes motivos para esses tipos de dano. Esses motivos podem incluir a atividade de programas maliciosos, configuração do sistema incorreta, falhas do sistema ou até a operação incorreta de aplicativos de otimização do sistema.

Depois de concluir a análise, o Assistente examina as informações a fim de avaliar se houve danos no sistema que exigem atenção imediata. Dependendo da análise, será gerada uma lista de ações necessárias para eliminar os problemas. O Assistente agrupa essas ações em categorias de acordo com a gravidade dos problemas detectados.

Para iniciar o Assistente de Solução de Problemas pós-infecção do Microsoft Windows:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Solução de Problemas do Microsoft Windows**, clique no botão **Iniciar**.

   A janela do Assistente de Solução de Problemas pós-infecção do Microsoft Windows é aberta.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Step 1. Iniciando a restauração do sistema

Confirme se a opção do Assistente para **Pesquisar problemas causados por atividade de malware** está selecionada e clique no botão **Avançar**.

Step 2. Pesquisa de problemas

O Assistente procurará problemas e danos que devem ser corrigidos. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionando as ações de solução de problemas

Todos os problemas encontrados na etapa anterior são agrupados de acordo com o tipo de perigo que representam. Para cada grupo de problemas, a Kaspersky Lab recomenda uma sequência de ações para reparar os danos. Há três grupos de ações:

- *Ações altamente recomendadas* eliminam os problemas que representam uma ameaça de segurança grave. É recomendável executar todas as ações desse grupo.
- *Ações recomendadas* eliminam os problemas que representam uma possível ameaça. Também é recomendável executar todas as ações desse grupo.
- *Ações adicionais* reparam danos ao sistema que não representam uma ameaça atual, mas que podem colocar a segurança do computador em perigo no futuro.

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Step 4. Corrigir problemas

O Assistente executará as ações selecionadas na etapa anterior. A correção de problemas poderá demorar algum tempo. Quando a solução de problemas for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o assistente.

VERIFICANDO EMAIL E FILTRANDO ANEXOS EM MENSAGENS DE EMAIL

O Kaspersky Internet Security permite a verificação de mensagens de email quanto à presença de objetos perigosos usando o Antivírus de Email. O Antivírus de Email é iniciado quando o sistema operacional é iniciado e permanece em execução permanente na RAM, verificando todas as mensagens de email enviadas ou recebidas através de POP3, SMTP, IMAP, MAPI e NNTP, bem como através de conexões criptografadas (SSL) através de POP3, SMTP e IMAP.

Por padrão, o Antivírus de Email verifica as mensagens enviadas e recebidas. Se necessário, você pode ativar a verificação somente das mensagens recebidas.

Para verificar somente as mensagens de mail recebidas:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
4. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Email** é aberta.
5. Na janela exibida, utilize a guia **Geral** na seção **Escopo de proteção** para selecionar a opção **Apenas mensagens recebidas**.

Caso não tenham sido detectadas ameaças em uma mensagem de email, ou caso todos os objetos infetados tenham sido desinfetados com êxito, a mensagem fica disponível para operações adicionais. Se o componente não conseguir desinfetar um objeto infetado, o Antivírus de Email renomeia ou exclui o objeto da mensagem e expande o assunto da mensagem com uma notificação que indica que a mensagem foi processada pelo Kaspersky Internet Security. Antes de excluir um objeto, o Kaspersky Internet Security cria uma cópia de backup dele e coloca a cópia na Quarentena (consulte a seção "Restaurar um arquivo excluído ou desinfetado pelo aplicativo" na página 32).

Os programas maliciosos podem se disseminar em mensagens de email. Você pode ativar a filtragem de anexos em mensagens de email. A filtragem permite a renomeação ou exclusão automática de arquivos de anexos dos tipos especificados.

Para ativar a filtragem de anexos em mensagens de email:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
4. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Email** é aberta.
5. Na janela exibida, na guia **Filtro de anexos**, selecione um modo de filtragem de anexos (**Renomear tipos de anexos selecionados** ou **Excluir tipos de anexos selecionados**).
6. A partir da lista de tipos de arquivo (extensões), selecione tipos de anexos que devem ser filtrados.

   Se desejar adicionar uma máscara de um novo tipo de arquivo:

   a. Clique no link **Adicionar** na parte inferior da janela para abrir a janela **Inserir máscara de nomes de arquivos**.

   b. Na janela exibida, insira uma máscara de tipo de arquivo.
7. Clique no botão **Aplicar** na janela **Configurações**.

BLOQUEANDO EMAIL INDESEJADO (SPAM)

Se você receber grandes quantidades de mensagens indesejadas (spam), ative o componente Antispam e defina o nível de segurança recomendado.

Para ativar o Antispam e definir o nível de segurança recomendado:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antispam**.
4. À direita da janela, marque a caixa **Ativar Antispam**.
5. Verifique se o nível de segurança **Recomendado** está definido na seção **Nível de segurança**.

   Se o nível de segurança for definido como **Baixo** ou **Personalizado**, clique no botão **Nível padrão**. O nível de segurança será automaticamente definido como **Recomendado**.

VERIFICAR O COMPUTADOR QUANTO À PRESENÇA DE VULNERABILIDADES

Vulnerabilidades são partes não protegidas do código do software que os invasores podem usar deliberadamente para atingir seus objetivos, como copiar os dados usados em aplicativos não protegidos. A verificação de vulnerabilidades no computador ajuda a descobrir esses pontos fracos. É recomendável remover as vulnerabilidades detectadas.

Para iniciar a verificação de vulnerabilidades na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
2. Na janela **Verificação** que é aberta, na seção **Verificação de Vulnerabilidades**, clique no botão .

PROCESSANDO APLICATIVOS DESCONHECIDOS

O Kaspersky Internet Security ajuda a minimizar o risco envolvido no uso de aplicativos desconhecidos (como o risco de infecção por vírus e alterações indesejadas às configurações do sistema operacional).

O Kaspersky Internet Security inclui componentes e ferramentas que permitem a verificação da reputação de um aplicativo e o controle das atividades realizadas no computador.

NESTA SEÇÃO

Verificar a reputação do aplicativo.....37

Controlando atividades de aplicativos no computador e na rede.....38

VERIFICAR A REPUTAÇÃO DO APLICATIVO

O Kaspersky Internet Security permite que você conheça a reputação de aplicativos dentre os usuários de todo o mundo. A reputação de um aplicativo compreende os seguintes critérios:

- nome do fornecedor;
- informações sobre a assinatura digital (disponíveis se houver uma assinatura digital);
- informações sobre o grupo no qual o aplicativo foi incluído pelo Controle de Aplicativos ou pela maioria dos usuários do Kaspersky Security Network;
- número de usuários do Kaspersky Security Network que usam o aplicativo (disponível se o aplicativo tiver sido incluído no grupo Confiável do banco de dados do Kaspersky Security Network);
- hora em que o aplicativo ficou conhecido no Kaspersky Security Network;
- países nos quais o aplicativo é mais disseminado.

A verificação de reputação do aplicativo está disponível caso você tenha acordado participar na Kaspersky Security Network.

Para saber a reputação de um aplicativo,

abra o menu de contexto do arquivo executável do aplicativo e selecione **Verificar a reputação no KSN** (consulte a imagem abaixo).

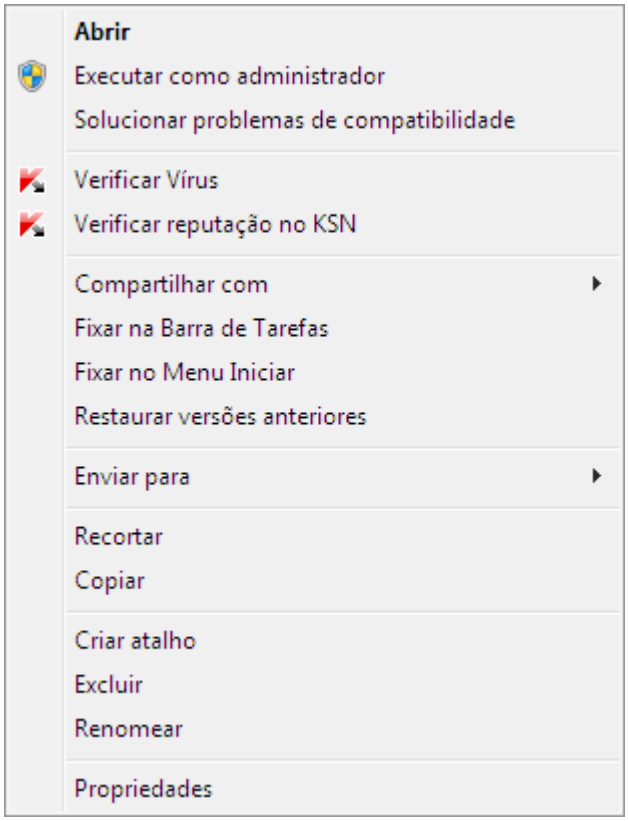

Figura 5. O menu de contexto de um objeto no Microsoft Windows

É exibida uma janela com informações sobre a reputação do aplicativo no KSN.

CONSULTE TAMBÉM:

A participação na Kaspersky Security Network (KSN).....60

CONTROLANDO ATIVIDADES DE APLICATIVOS NO COMPUTADOR E NA REDE

O Controle de Aplicativos evita que aplicativos executem ações que podem ser perigosas para o sistema e garante o controle do acesso aos recursos do sistema operacional e seus dados de identidade.

O componente rastreia as ações executadas no sistema por aplicativos instalados no computador e os administra com base nas regras do Controle de Aplicativos. Essas regras gerenciam atividades possivelmente perigosas, incluindo o acesso de aplicativos a recursos protegidos, como arquivos e pastas, chaves do Registro e endereços de rede.

A atividade de rede dos aplicativos é controlada pelo componente Firewall.

Quando um aplicativo é executado pela primeira vez no computador, o Controlo de Aplicativos verifica a segurança e move o aplicativo para um dos grupos: (**Confiável**, **Não confiável**, **Alta restrição** ou **Baixa restrição**). O grupo define as regras que deverão ser aplicadas pelo Kaspersky Internet Security para controlar a atividade desse aplicativo.

Você pode editar as regras do controle de aplicativos manualmente.

Para editar as regras de aplicativos manualmente:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, selecione a subseção **Controle de Aplicativos** na seção **Centro de Proteção**.
4. À direita da janela, na seção **Configurar regras de aplicativos, proteger dados de identidade digital e outros recursos**, clique no botão **Aplicativos**.
5. Na janela **Aplicativos** que é aberta, selecione o aplicativo desejado na lista e clique no botão **Editar**.
6. Na janela **Regras de aplicativos** que é aberta, configure as regras de aplicativos:
   - Para configurar regras de acesso aos recursos do sistema operacional para um aplicativo:
     a. Na guia **Registro do sistema e arquivos** selecione a categoria de recurso necessária.
     b. Clique com o botão direito na coluna com uma ação disponível no recurso (**Ler**, **Gravar**, **Excluir** ou **Criar**) para abrir o menu de contexto e selecionar o valor necessário (**Permitir**, **Bloquear** ou **Perguntar o que fazer**).
   - Para configurar os direitos de um aplicativo para realizar várias ações no sistema operacional:
     a. Na guia **Direitos**, selecione a categoria necessária de direitos.
     b. Clique com o botão direito na coluna **Permissão** para abrir o menu de contexto e selecione o valor necessário (**Permitir**, **Bloquear** ou **Perguntar o que fazer**).

- Para configurar os direitos de um aplicativo para realizar várias ações na rede:

  a. Na guia **Regras de rede**, clique no botão **Adicionar**.

     A janela **Regra de rede** é exibida.

  b. Na janela que é exibida, especifique as configurações desejadas e clique no botão **OK**.

  c. Atribua uma prioridade à nova regra usando os botões **Mover para cima** e **Mover para baixo** para movê-la para cima ou para baixo na lista.

- Para excluir algumas ações do escopo do Controle de Aplicativos, na guia **Exclusões**, selecione as caixas de seleção que não devem ser controladas.

  Todas as exclusões criadas nas regras para aplicativos do usuário podem ser acessadas na janela de configurações do aplicativo, na seção **Ameaças e Exclusões**.

7. Clique no botão **Aplicar** na janela **Configurações**.

PROTEGENDO DADOS PARTICULARES CONTRA ROUBO

O Kaspersky Internet Security ajuda você a proteger seus dados particulares contra roubo:

- senhas, nomes de usuário e outros dados de registro;
- números de contas e cartões bancários.

O Kaspersky Internet Security inclui componentes e ferramentas que permitem proteger seus dados particulares contra tentativas de roubo por hackers, os quais usam métodos como o phishing e a intercepção de dados inseridos com o teclado.

A proteção contra phishing é garantida pelo Antiphishing implementado nos componentes Antivírus da Web, Antispam e Antivírus de IM.

A proteção contra a intercepção de dados inseridos com o teclado é fornecida pelo Teclado Virtual e pela proteção dos dados inseridos com o teclado do computador.

O Assistente de Limpeza de Dados foi concebido para limpar todas as informações no computador sobre as atividades do usuário.

A proteção de dados ao usar os serviços de banco virtual da Internet e lojas virtuais é fornecida pelos recursos da Banca Segura.

A proteção contra a transferência de dados particulares através da Internet é fornecida por uma ferramenta do Controle para Pais (consulte a seção "Aplicando o Controle para Pais a usuários do computador" na página 48).

NESTA SEÇÃO

Proteção contra phishing 40

Teclado Virtual 40

Proteção da inserção de dados com o teclado do computador 43

Banca Segura 44

Limpeza de Dados Particulares 45

PROTEÇÃO CONTRA PHISHING

A proteção contra phishing é garantida pelo Antiphishing implementado nos componentes Antivírus da Web, Antispam e Antivírus de IM. Ative esses componentes para garantir uma proteção completa contra phishing.

Você pode definir as configurações adicionais de antiphishing nos componentes Antivírus da Web e Antivírus de IM.

Para configurar a proteção de antiphishing quando o Antivírus da Web está sendo executado:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, vá à seção **Proteção**, selecione a subseção **Antivírus da Web** e clique no botão **Configurações**.

   A janela **Antivírus da Web** é aberta.
4. Na janela que é aberta, na guia **Geral**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar páginas da Web quanto à presença de phishing**.
5. Se desejar que o Antiphishing use análise heurística clique no botão **Adicionais** ao verificar páginas da Web.

   A janela **Configurações do Antiphishing** é exibida.
6. Na janela exibida, marque a caixa **Usar a Análise Heurística para verificar páginas da Web quanto à presença de phishing** e defina o nível de detalhamento da verificação.
7. Clique no botão **Aplicar** na janela **Configurações**.

Para configurar a proteção de anti-phishing para usar durante o funcionamento do Antivírus de IM:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, selecione a subseção **Antivírus de IM** na seção **Centro de Proteção**.
4. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Verificar se os URLs estão listados no banco de dados de URLs de phishing**.
5. Clique no botão **Aplicar** na janela **Configurações**.

TECLADO VIRTUAL

Ao trabalhar na Internet, frequentemente você precisa inserir seus dados pessoais ou seu nome de usuário e sua senha. Isso acontece, por exemplo, ao registrar uma conta em sites, fazer compras online ou usar um banco virtual.

Existe um risco de que essas informações pessoais sejam interceptadas usando interceptadores de teclado ou keyloggers, que são programas que registram o pressionamento de teclas.

A ferramenta Teclado Virtual evita a interceptação dos dados inseridos usando o teclado.

O Teclado Virtual evita apenas a interceptação de dados particulares ao trabalhar com os navegadores Microsoft Internet Explorer, Mozilla™ Firefox™ e Google Chrome™. Quando usado junto com outros navegadores, o Teclado Virtual não protege dados particulares inseridos contra a intercepção.

O Teclado Virtual não poderá proteger seus dados pessoais se o site que exibe a inserção desses dados tiver sido invadido; nesse caso, as informações são obtidas diretamente pelos invasores.

Muitos programas classificados como spyware podem tirar capturas de ecrã, as quais são automaticamente transmitidas a um intruso para análise futura e para roubar os dados particulares do usuário. O Teclado Virtual evita que os dados particulares inseridos sejam interceptados por meio de capturas de tela.

O Teclado Virtual não impede que sejam feitas capturas de tela através da tecla Print Screen ou de outras combinações de teclas fornecidas pelas configurações do sistema operacional, nem de capturas de tela através do DirectX.

O Teclado Virtual possui os seguintes recursos:

- Você pode clicar nos botões do Teclado Virtual usando o mouse.
- Diferentemente dos teclados reais, no Teclado Virtual não é possível clicar em várias teclas simultaneamente. É por isso que usar combinações de teclas (como **ALT**+**F4**) requer que o usuário pressione a primeira tecla (por exemplo, **ALT**), depois a segunda tecla (por exemplo, **F4**) e novamente a primeira tecla. O segundo clique na tecla funciona da mesma forma que a liberação da mesma em um teclado real.
- O idioma do Teclado Virtual pode ser alterado usando o mesmo atalho especificado nas configurações do sistema operacional para o teclado físico. É necessário clicar com o botão direito na outra tecla (por exemplo, se o atalho **LEFT ALT**+**SHIFT** estiver definido nas configurações do sistema operacional para mudar o idioma do teclado, é necessário clicar com o botão esquerdo na tecla **LEFT ALT** e com o botão direito na tecla **SHIFT**).

Para garantir a proteção de dados inseridos no Teclado Virtual, reinicie o computador após a instalação do Kaspersky Internet Security.

Você pode abrir o Teclado Virtual das seguintes formas:

- a partir do menu de contexto do ícone de aplicativo, na área de notificações da barra de tarefas;
- na janela principal do aplicativo;
- nas janelas dos navegadores Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome;
- usando o ícone de início rápido do Teclado Virtual em campos de entrada de sites;

  Você pode configurar a exibição do ícone de início rápido em campos de entrada em sites.

- usando uma combinação de teclas no teclado do computador;
- usando o Gadget do Kaspersky Internet Security (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).

- *Para abrir o Teclado Virtual no menu de contexto do ícone do aplicativo na área de notificações da barra de tarefas,*

  selecione **Ferramentas → Teclado Virtual** no menu de contexto do ícone do aplicativo (consulte a figura abaixo).

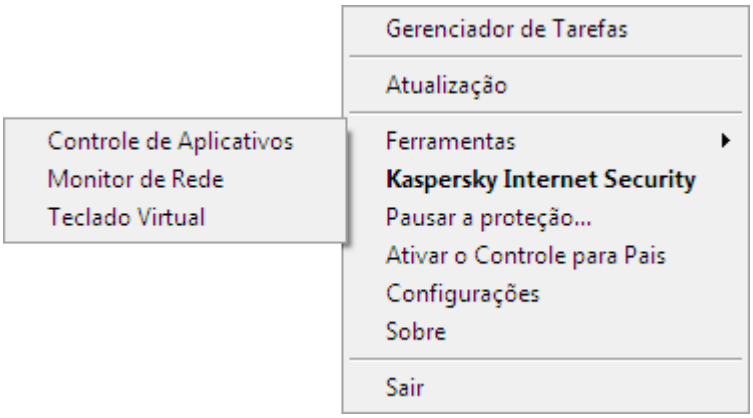

Figura 6. Menu de contexto do ícone do aplicativo

- *Para abrir o Teclado Virtual na janela principal do aplicativo,*

  na parte inferior da janela principal do aplicativo, selecione a seção **Teclado Virtual**.

- *Para abrir o Teclado Virtual na janela do navegador,*

  clique no botão **Teclado Virtual** na barra de ferramentas do Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome.

- *Para abrir o Teclado Virtual usando o teclado do computador,*

  pressione o atalho **CTRL+ALT+SHIFT+P**.

- *Para abrir o Teclado Virtual usando o gadget,*

  clique no botão do gadget ao qual a ação foi atribuída (consulte a seção "Usando o Kaspersky Gadget" na página 58).

- *Para configurar a exibição do ícone de início rápido do Teclado Virtual em campos de entrada de sites:*

  1. Abra a janela principal do aplicativo.
  2. Na parte superior da janela, clique no link **Configurações**.
  3. Na janela **Configurações** que é exibida, na seção **Centro de Proteção**, selecione a subseção **Inserção de dados segura com o teclado**.
  4. À direita da janela, na seção **Teclado Virtual** selecione a caixa de seleção **Exibir ícone de iniciação rápida em campos de inserção de dados** e clique no botão **Configurações**.

     A janela **Teclado Virtual** é exibida.
  5. Na janela exibida, configure regras para a exibição do ícone de início rápido:

     - Na guia **Categorias** selecione as caixas de seleção para as categorias de sites em que o ícone de início rápido deve ser exibido nos campos de entrada.
     - Se desejar que o ícone de início rápido seja exibido nos campos de entrada de sites abertos em Execução Segura de Sites durante a utilização da Banca Segura, na guia **Categorias** selecione a caixa de seleção **Exibir ícone de início rápido do Teclado Virtual em campos da Banca Segura**.

- Se desejar ativar a exibição do ícone de início rápido em campos de entrada de um sites específico:

  a. Na guia **Exclusões**, na lista **Exibir ícone de início rápido em sites** clique no botão **Adicionar**.

     A janela **Exibir ícone de início rápido** é aberta.

  b. Na janela exibida, insira o URL de um site no campo **URL** e selecione uma das opções de exibição do ícone de início rápido nesse site (**Exibir ícone somente na página da Web especificada** ou **Exibir ícone em todo o site**).

6. Clique no botão **Aplicar** na janela **Configurações**.

PROTEÇÃO DA INSERÇÃO DE DADOS COM O TECLADO DO COMPUTADOR

Ao trabalhar na Internet, frequentemente você precisa inserir seus dados pessoais ou seu nome de usuário e sua senha. Isso acontece, por exemplo, ao registrar uma conta em sites, fazer compras online ou usar um banco virtual.

Existe um risco de que essas informações pessoais sejam interceptadas usando interceptadores de teclado ou keyloggers, que são programas que registram o pressionamento de teclas.

A proteção da inserção de dados com o teclado do computador permite evitar a intercepção de dados inseridos com o teclado.

A proteção da inserção de dados com o teclado do computador está disponível somente para os navegadores Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Ao usar outros navegadores da Web, os dados inseridos com o teclado do computador não são protegidos contra intercepção.

A proteção da inserção de dados com o teclado do computador não protege seus dados particulares caso um site que requeira a inserção desses dados tenha sido alvo de ataque, uma vez que nesse caso as informações serão enviadas diretamente para os invasores.

Você pode configurar a proteção da inserção de dados com o teclado do computador em vários sites. Após a proteção da inserção de dados com o teclado do computador ter sido configurada, você não terá de executar quaisquer ações adicionais ao inserir dados.

Para proteger dados inseridos com o teclado do computador, reinicie o computador após a instalação do Kaspersky Internet Security.

Para configurar a proteção da inserção de dados com o teclado do computador:

1. Abra a janela principal do aplicativo.

2. Na parte superior da janela, clique no link **Configurações**.

3. Na janela **Configurações** que é exibida, na seção **Centro de Proteção**, selecione a subseção **Inserção de dados segura com o teclado**.

4. À direita da janela, na seção **Inserção de dados segura com o teclado**, marque a caixa **Ativar a inserção de dados segura com o teclado** e clique no botão **Configurações**.

   A janela **Inserção de dados segura com o teclado** é exibida.

5. Na janela exibida, especifique o escopo de proteção para a inserção de dados com o teclado do computador:

   - Na guia **Categorias**, selecione as caixas de seleção para as categorias de sites em que os dados inseridos com o teclado devem ser protegidos.

- Se desejar que a inserção de dados com o teclado seja protegida em sites abertos no modo Execução Segura de Sites com a Banca Segura, na guia **Categorias**, selecione a caixa de seleção **Ativar a inserção de dados segura com o teclado para a Banca Segura**.

- Se desejar que a inserção de dados com o teclado seja protegida em campos de senha em todos os sites, na guia **Categorias**, selecione a caixa de seleção **Proteger campos de senha em todos os sites**.

- Se desejar ativar a proteção da inserção de dados com o teclado em um site especificado:

  a. Na guia **Exclusões**, na lista **Ativar a inserção de dados segura com o teclado em sites**, clique no botão **Adicionar**.

     A janela **Site protegido** é exibida.

  b. Na janela exibida, insira o URL de um site no campo **URL** e selecione uma das opções de proteção para a inserção de dados nesse site (**Ativar a proteção somente na página da Web especificada** ou **Ativar a proteção em todo o site**).

6. Clique no botão **Aplicar** na janela **Configurações**.

BANCA SEGURA

Para fornecer proteção para os dados confidenciais que inserir em sites de bancos e sistemas de pagamento (como números de cartões de crédito e senhas para acessar serviços bancários online), bem como para impedir o roubo de ativos quando efetuar pagamentos online, o Kaspersky Internet Security solicita que abra esses sites na Execução Segura de Sites.

A Execução Segura de Sites não pode ser executada se a caixa de seleção **Ativar Autodefesa** estiver selecionada na seção **Configurações Avançadas**, na subseção **Autodefesa** da janela de configurações do aplicativo.

Você pode configurar a Banca Segura de modo a que o aplicativo reconheça automaticamente sites de bancos e sistemas de pagamento.

Para configurar a Banca Segura:

1. Abra a janela principal do aplicativo.

2. Na parte superior da janela, clique no link **Configurações**.

3. Na janela **Configurações** que é exibida, na seção **Centro de Proteção**, selecione a subseção **Banca Segura**.

4. Selecione a caixa de seleção **Ativar a Banca Segura**.

5. Para ativar a notificação das vulnerabilidades detectadas no sistema operacional antes de iniciar a Execução Segura de Sites, selecione a caixa de seleção **Notificar sobre vulnerabilidades do sistema operacional**.

6. Para configurar a Banca Segura para um site específico:

   a. Na lista **Sites de bancos e sistemas de pagamento**, clique no botão **Adicionar**.

      A janela **Site da Banca Segura** é exibida.

   b. Na janela exibida, no campo **Site de banco ou sistema de pagamento**, insira o URL de um site que deva ser aberto na Execução Segura de Sites.

      O URL de um site deve ser antecedido do prefixo de protocolo https:// usado pela Execução Segura de Sites por padrão.

   c. Se necessário, no campo **Descrição**, insira o nome ou uma descrição desse site.

d. Selecione um método para iniciar a Execução Segura de Sites ao abrir o site:

- Se desejar que o Kaspersky Internet Security solicite o início da Execução Segura de Sites sempre que abrir o site, selecione **Perguntar o que fazer**.
- Se desejar que o Kaspersky Internet Security abra automaticamente o site no modo Execução Segura de Sites, selecione **Executar o navegador protegido automaticamente**.
- Se desejar desativar a Banca Segura para o site, selecione **Não executar o navegador protegido**.

7. Clique no botão **Aplicar** na janela **Configurações**.

LIMPEZA DE DADOS PARTICULARES

As ações do usuário em um computador são registradas no sistema operacional. São salvas as seguintes informações:

- detalhes de consultas de pesquisa inseridas por usuários e sites visitados
- informações sobre os aplicativos iniciados, arquivos abertos e salvos;
- entradas de log de eventos do Microsoft Windows;
- outras informações da atividade do usuário.

As informações sobre ações do usuário que contenham informações confidenciais podem ficar disponíveis para invasores e pessoas não autorizadas.

O Kaspersky Internet Security inclui o Assistente de Limpeza de Dados Particulares que limpa os rastros de atividade do usuário no sistema.

Para iniciar o Assistente de Limpeza de Dados Particulares:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Limpeza de Dados Particulares**, clique no botão **Iniciar**.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Step 1. Iniciando o Assistente

Confirme se a opção **Pesquisar rastros de atividades de usuários** está selecionada e clique no botão **Avançar** para iniciar o Assistente.

Step 2. Pesquisa de sinais de atividade

Este assistente pesquisa rastros de atividades de malware no computador. A pesquisa poderá demorar algum tempo. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionando ações de Limpeza de Dados Particulares

Ao concluir a pesquisa, o Assistente exibe os rastros de atividades detectados e as ações sugeridas para eliminá-los (consulte a figura abaixo).

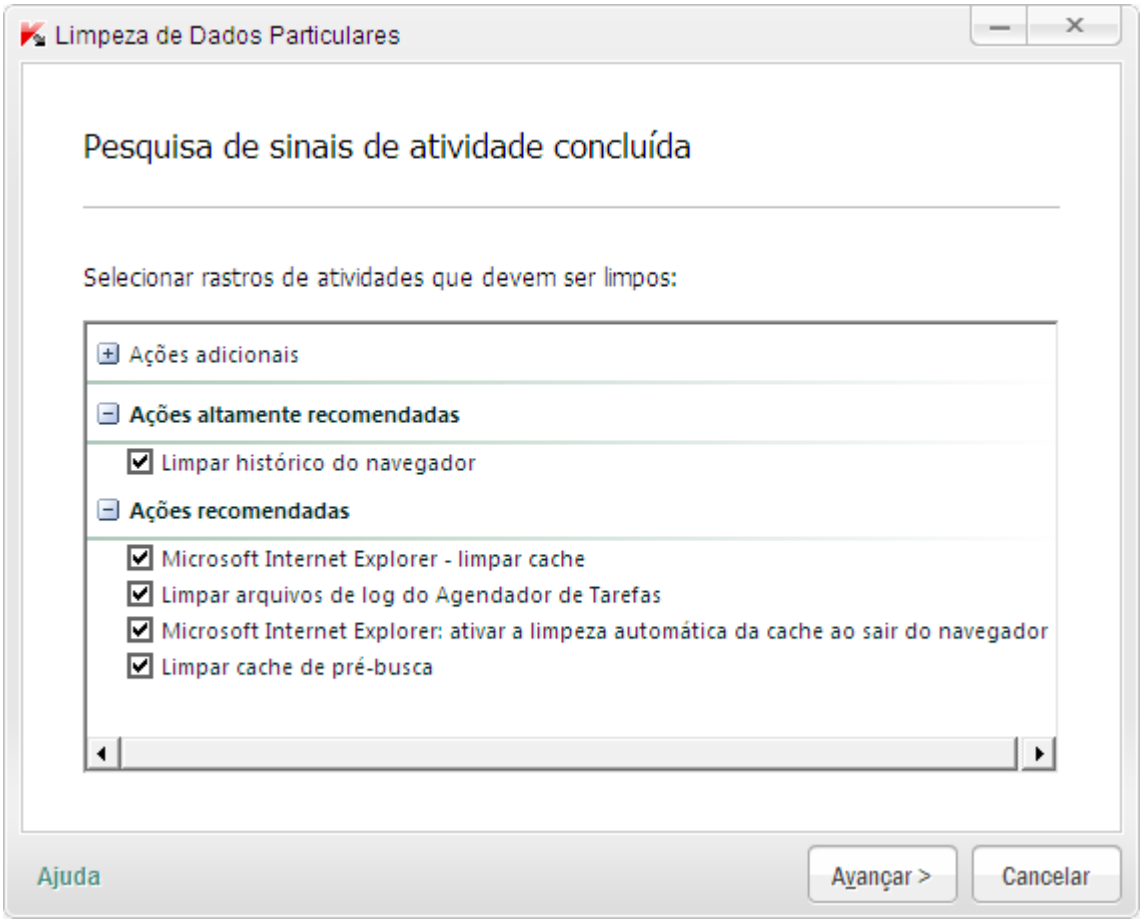
Limpeza de Dados Particulares
Pesquisa de sinais de atividade concluída
Selecionar rastros de atividades que devem ser limpos:
Ações adicionais
Ações altamente recomendadas
Limpar histórico do navegador
Ações recomendadas
Microsoft Internet Explorer - limpar cache
Limpar arquivos de log do Agendador de Tarefas
Microsoft Internet Explorer: ativar a limpeza automática da cache ao sair do navegador
Limpar cache de pré-busca
Ajuda
Avançar >
Cancelar

Figura 7. Rastros de atividades detectados e recomendações sobre como eliminá-los

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

Limpar as caixas de seleção selecionadas por padrão não é recomendável. Isso pode comprometer a segurança do computador.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Step 4. Limpeza de Dados Particulares

O Assistente executará as ações selecionadas na etapa anterior. A eliminação dos rastros de atividades pode levar algum tempo. Para limpar determinados rastros de atividades, talvez seja necessário reiniciar; se for o caso, o Assistente o notificará.

Quando a limpeza for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 5. Conclusão do Assistente

Se desejar limpar os rastros de atividades do usuário automaticamente sempre que o Kaspersky Internet Security concluir seu trabalho, na última tela do Assistente, marque a caixa **Limpar rastros de atividades sempre ao sair do Kaspersky Internet Security**. Se desejar remover os rastros de atividades manualmente usando o Assistente, não marque essa caixa.

Clique no botão **Concluir** para fechar o assistente.

AVALIANDO O STATUS DE SEGURANÇA DE UM SITE

O Kaspersky Internet Security permite a verificação de um site quanto à segurança antes de acessar esse site através de um link. Para isso, é usado um módulo nomeado *Consultor de URLs da Kaspersky*.

O Consultor de URLs da Kaspersky é integrado nos navegadores Microsoft Internet Explorer, Google Chrome e Mozilla Firefox, verificando os links em páginas da Web abertas no navegador. O Kaspersky Internet Security exibe um dos seguintes ícones junto a cada link:

- – se a página da Web aberta clicando no link for segura, de acordo com a Kaspersky Lab
- – se não existirem informações sobre o status de segurança da página da Web aberta ao clicar no link
- – se a página da Web aberta clicando no link for perigosa, de acordo com a Kaspersky Lab.

Ao passar o ponteiro do mouse sobre um ícone, é exibida uma janela pop-up com mais detalhes sobre o link.

Por padrão, o Kaspersky Internet Security verifica links somente em resultados de pesquisa. Você pode ativar a verificação de links no site inteiro.

Para ativar a verificação de links no site inteiro:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, vá à seção **Proteção**, selecione a subseção **Antivírus da Web** e clique no botão **Configurações**.

   A janela **Antivírus da Web** é aberta.
4. Na janela aberta, na guia **Filtro da Web**, na seção **Consultor de URLs Kaspersky**, clique no botão **Configurações**.

   É exibida a janela **Configurações do Consultor de URLs Kaspersky**.
5. Na janela exibida, na seção **Modo de Verificação**, selecione **Todos os URLs**.
6. Clique no botão **Aplicar** na janela **Configurações**.

BLOQUEANDO O ACESSO A SITES DE VÁRIAS REGIÕES

De acordo com estatísticas coletadas pela Kaspersky Lab, as taxas de infecção de sites podem variar dependendo do país de origem. O Kaspersky Internet Security usa um componente designado Filtro Geográfico para bloquear o acesso a sites que pertencem a domínios regionais especificados com altas taxas de infecção.

Quando o Filtro Geográfico é ativado, o Kaspersky Internet Security permite ou bloqueia o acesso a um domínio regional ou solicita permissão de acesso ao usuário, dependendo da definição.

Para ativar e configurar o Filtro Geográfico:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, vá à seção **Proteção**, selecione a subseção **Antivírus da Web** e clique no botão **Configurações**.

   A janela **Antivírus da Web** é aberta.
4. Na janela exibida, na guia **Filtro Geográfico**, selecione a caixa **Ativar a filtragem por domínios regionais**.
5. Na parte inferior da janela, na lista de domínios controlados, especifique os domínios aos quais o acesso deve ser permitido ou bloqueado, ou especifique os domínios que requerem um pedido de permissão de acesso.
6. Clique no botão **Aplicar** na janela **Configurações**.

APLICANDO O CONTROLE PARA PAIS A USUÁRIOS DO COMPUTADOR

O *Controle para Pais* permite monitorar as ações executadas por usuário no computador e online. O Controle para Pais oferece a opção de restringir o acesso a aplicativos e recursos da Internet, além de exibir relatórios das atividades dos usuários.

Atualmente, um número cada vez maior de crianças e adolescentes tem acesso a computadores e recursos da Web. O uso de computadores e da Internet expõe as crianças a um conjunto de riscos:

- perda de tempo e/ou dinheiro ao visitar salas de bate-papo, recursos de jogos, lojas virtuais, leilões;
- acesso a sites destinados ao público adulto, como aqueles que exibem pornografia, extremismos, armas de fogo, abuso de drogas e violência explícita;
- download de arquivos infectados com malware;
- danos de saúde causados pelo uso excessivo do computador;
- contatos com pessoas desconhecidas que podem fingir ser colegas para obter informações pessoais de usuários menores, como nomes reais, endereços físicos, horários do dia em que não há pessoas em casa.

O Controle para Pais permite reduzir os riscos impostos pelo computador e pela Internet. Para fazer isso, as seguintes funções do módulo são usadas:

- limitar o tempo de uso do computador e da Internet;
- criar listas de aplicativos permitidos e bloqueados, além de limitar temporariamente o número de execuções dos aplicativos permitidos;
- criar listas de sites permitidos e bloqueados, e selecionar as categorias de sites com conteúdo não recomendável para exibição;
- ativar o modo de pesquisa segura em mecanismos de pesquisa (os links para sites com conteúdo suspeito não são exibidos nos resultados da pesquisa);
- restringir downloads de arquivos da Internet;
- criar listas de contatos que são permitidos ou bloqueados para a comunicação através de programas de IM e redes sociais;

- exibir logs de mensagens de programas de IM e redes sociais;
- bloquear o envio de determinados dados pessoais;
- procurar determinadas palavras-chave em logs de mensagens.

Todas essas restrições podem ser ativadas de forma independente, o que permite configurar o Controle para Pais de forma flexível para vários usuários. Para cada conta, você pode exibir relatórios dos eventos das categorias que devem ser controladas que o componente registrou durante o período especificado.

NESTA SEÇÃO

Configurando o Controle para Pais.....49

Exibindo o relatório de atividade de um usuário.....49

CONFIGURANDO O CONTROLE PARA PAIS

Caso não tenha acesso protegido às configurações do Kaspersky Internet Security com uma senha, na primeira inicialização do Controle para Pais, o Kaspersky Internet Security irá sugerir que você configure uma senha para impedir alterações não autorizadas às configurações do controle. Em seguida, você pode configurar restrições ao uso do computador e da Internet em todas as contas do computador.

Para configurar o Controle para Pais em uma conta:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Controle para Pais**.
3. Na janela que é aberta, na seção que contém a conta, clique no botão .

   A janela **Controle para Pais** é exibida.
4. Na janela que é exibida, na guia **Configurações**, selecione o tipo de restrição na parte esquerda da janela e especifique as configurações do controle na parte direita da janela.
5. Clique no botão **OK** na janela **Controle para Pais** para salvar as configurações de controle que selecionou.

EXIBINDO O RELATÓRIO DE ATIVIDADE DE UM USUÁRIO

Você pode acessar os relatórios de atividades de cada conta de usuário no Controle para Pais, examinando individualmente cada categoria de eventos controlados.

Para exibir o relatório de atividades de uma conta de usuário controlada:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Controle para Pais**.
3. Na janela que é aberta, na seção que contém a conta, clique no botão .

   A janela **Controle para Pais** é exibida.

4. Selecione a guia **Relatórios**.

5. À esquerda da janela que é aberta, selecione a categoria de operações ou conteúdo controlado, como **Uso da Internet** ou **Dados Particulares**.

   Um relatório de ações e conteúdo controlados será exibido à direita da janela.

USANDO O PERFIL DE JOGO PARA MODO DE TELA INTEIRA

Quando o Kaspersky Internet Security está sendo executado em simultâneo com alguns aplicativos (em particular, jogos de vídeo), podem ocorrer os seguintes problemas no modo de tela inteira:

- O desempenho do aplicativo ou do jogo diminui, devido à falta de recursos do sistema
- As janelas de notificação do Kaspersky Internet Security distraem o usuário do jogo.

Para evitar alterar as configurações do Kaspersky Internet Security manualmente sempre que mudar para o modo de tela inteira, pode usar o Perfil de Jogo. Quando o Perfil de Jogo está ativo, ao alternar para o modo de tela inteira, as configurações de todos os componentes do Kaspersky Internet Security são alteradas automaticamente para assegurar o funcionamento ideal do sistema nesse modo. Ao sair do modo de tela inteira, as configurações do produto retornam aos valores iniciais usados antes de entrar nesse modo.

Para ativar o Perfil de Jogo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Perfil de Jogo**.
3. Selecione a caixa **Usar Perfil de Jogo** e, na seção **Opções do perfil** abaixo, especifique as configurações de perfil de jogo desejadas.

CRIAR E USAR O DISCO DE RECUPERAÇÃO

O Disco de Recuperação consiste em um aplicativo denominado Kaspersky Rescue Disk e gravado em uma mídia removível (CD ou unidade flash USB).

Você pode usar o Kaspersky Rescue Disk para verificar e desinfetar computadores infetados que não podem ser desinfetados usando outros métodos (por exemplo, com aplicativos antivírus).

NESTA SEÇÃO

Criando um Disco de Recuperação 50

Inicializando o computador com o Disco de Recuperação 52

CRIANDO UM DISCO DE RECUPERAÇÃO

A criação de um Disco de Recuperação consiste em criar uma imagem do disco (arquivo ISO) com a versão atualizada do Kaspersky Rescue Disk e gravá-la em uma mídia removível.

Você pode baixar a imagem original do disco do servidor da Kaspersky Lab ou copiá-la de uma fonte local.

O Disco de Recuperação é criado usando o *Assistente para Criação do Kaspersky Rescue Disk*. O arquivo rescuecd.iso criado pelo Assistente é salvo no disco rígido do computador:

- no Microsoft Windows XP – na seguinte pasta: Documents and Settings\All Users\Dados de Aplicativos\Kaspersky Lab\AVP13\Data\Rdisk\;
- nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7 – na seguinte pasta: ProgramData\Kaspersky Lab\AVP13\Data\Rdisk\.

Para iniciar o Assistente para Criação do Kaspersky Rescue Disk:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Kaspersky Rescue Disk**, clique no botão **Criar**.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Step 1. Iniciando o Assistente. Pesquisando uma imagem de disco existente

A primeira janela do Assistente contém informações sobre o Kaspersky Rescue Disk.

Se o Assistente detectar um arquivo ISO do Disco de Recuperação existente na pasta exclusiva (veja acima), a caixa **Usar imagem ISO existente** será exibida na primeira janela do Assistente. Marque a caixa para usar o arquivo detectado como a imagem ISO original e vá diretamente para a etapa **Atualizando imagem do disco** (veja a seguir). Desmarque esta caixa se não desejar usar a imagem do disco que foi detectada. O Assistente continuará na janela **Selecionar fonte da imagem do disco**.

Step 2. Selecionando a origem da imagem do disco

Se você marcou a caixa de seleção **Usar imagem do Kaspersky Rescue Disk existente** na primeira janela do Assistente, esta etapa será ignorada.

Nesta etapa, você deve selecionar a fonte da imagem do disco dentre as opções sugeridas:

- Se você já tiver uma cópia gravada do Disco de Recuperação ou uma imagem ISO salva no computador ou em um recurso de rede local, selecione **Copiar a imagem ISO da unidade local ou de rede**.
- Se você não tiver um arquivo de imagem ISO criado para o Disco de Recuperação e desejar baixá-lo do servidor da Kaspersky Lab (o tamanho do arquivo é aproximadamente 175 MB), selecione **Baixar a imagem ISO do servidor da Kaspersky Lab**.

Step 3. Copiando (baixando) a imagem do disco

Se você marcou a caixa de seleção **Usar imagem do Kaspersky Rescue Disk existente** na primeira janela do Assistente, esta etapa será ignorada.

Se você tiver selecionado **Copiar a imagem ISO da unidade local ou de rede** na etapa anterior, clique no botão **Procurar**. Depois de especificar o caminho do arquivo, clique no botão **Avançar**. O andamento da cópia da imagem do disco será exibido na janela do Assistente.

Se você selecionou **Baixar a imagem ISO do servidor da Kaspersky Lab**, o andamento do download da imagem do disco será exibido imediatamente.

Quando a cópia ou o download da imagem ISO for concluído, o Assistente continuará automaticamente na etapa seguinte.

Step 4. Atualizando o arquivo da imagem ISO

O procedimento de atualização do arquivo da imagem ISO compreende as seguintes operações:

- atualização dos bancos de dados do aplicativo
- atualização dos arquivos de configuração.

Os arquivos de configuração determinam se o computador pode ser inicializado a partir de uma mídia removível (como um CD/DVD ou uma unidade flash USB com o Kaspersky Rescue Disk) criada pelo Assistente.

Ao atualizar os bancos de dados do aplicativo, são usados aqueles distribuídos na última atualização do Kaspersky Internet Security. Se os bancos de dados estiverem desatualizados, é recomendável executar a tarefa de atualização e executar o Assistente para Criação do Kaspersky Rescue Disk novamente.

Para iniciar a atualização do arquivo ISO, clique no botão **Avançar**. O andamento da atualização será exibido na janela do Assistente.

Step 5. Gravando a imagem do disco em uma mídia

Nesta etapa, o Assistente informa sobre a criação bem-sucedida de uma imagem do disco e permite sua gravação em uma mídia.

Especifique uma mídia de dados para gravar o Kaspersky Rescue Disk:

- Para gravar a imagem do disco em um CD/DVD, selecione **Gravar em CD/DVD** e especifique a mídia na qual você deseja gravar a imagem do disco.
- Para gravar a imagem do disco em uma unidade flash USB, selecione **Gravar na unidade flash USB** e especifique o dispositivo no qual você deseja gravar a imagem do disco.

  A Kaspersky Lab recomenda não gravar a imagem ISO em dispositivos que não foram criados especificamente para armazenamento de dados, como smartphones, celulares, PDAs e MP3 players. Depois de ser usados para armazenar a imagem de disco, alguns dispositivos podem ter problemas de funcionamento.

- Para gravar a imagem do disco no disco rígido do computador ou de outro computador que você possa acessar através de uma rede, selecione **Salvar a imagem do disco em arquivo na unidade local ou de rede** e especifique a pasta na qual você deseja gravar a imagem do disco e o nome do arquivo ISO.

Step 6. Conclusão do Assistente

Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Você poderá usar o Disco de Recuperação recém criado para iniciar o computador (veja a página 52) caso não seja possível inicializá-lo e executar o Kaspersky Internet Security no modo normal devido ao impacto causado por vírus ou malware.

INICIALIZANDO O COMPUTADOR COM O DISCO DE RECUPERAÇÃO

Se não for possível iniciar o sistema operacional devido a um ataque de vírus, use o Disco de Recuperação.

Para iniciar o sistema operacional, você deve usar um CD/DVD ou uma unidade flash USB com o Kaspersky Rescue Disk gravado (consulte a seção "Criando um Disco de Recuperação" na página 50).

Nem sempre é possível iniciar o computador a partir de uma mídia removível. Especificamente, não há suporte para esse modo em alguns modelos de computador obsoletos. Antes de desligar o computador para a inicialização posterior a partir de uma mídia removível, verifique se essa operação pode ser executada.

Para inicializar o computador com o Disco de Recuperação:

1. Nas configurações do BIOS, ative a inicialização a partir do CD/DVD ou do dispositivo USB (para obter informações detalhadas, consulte a documentação da placa mãe do computador).

2. Insira um CD/DVD na unidade correspondente do computador infectado ou conecte um dispositivo flash USB com o Kaspersky Rescue Disk copiado.

3. Reinicie o computador.

Para obter informações detalhadas sobre o uso do Disco de Recuperação, consulte o Manual do Usuário do Kaspersky Rescue Disk.

PROTEGENDO POR SENHA O ACESSO AO KASPERSKY INTERNET SECURITY

Um único computador pode ser compartilhado entre diversos usuários com níveis de experiência em computação diferentes. O acesso não restringido de diferentes usuários ao Kaspersky Internet Security e suas configurações pode comprometer o nível de segurança do computador.

Para restringir o acesso ao aplicativo, é possível definir a senha de administrador e especificar as ações que exigem a inserção da senha:

- definindo as configurações do aplicativo;
- gerenciar o Controle para Pais;
- encerrar o aplicativo;
- remover o aplicativo.

Para proteger por senha o acesso ao Kaspersky Internet Security:

1. Abra a janela principal do aplicativo.

2. No canto superior direito da janela, clique no link **Configurações**.

3. Na janela **Configurações** que é exibida, selecione a subseção **Configurações Gerais** na seção **Centro de Proteção**.

4. Selecione a caixa de seleção **Ativar proteção por senha** e clique no botão **Configurações**.

   É aberta a janela **Proteção por senha**.

5. Na janela aberta, preencha os campos **Nova senha** e **Confirmar senha**.

6. Para alterar uma senha criada antes, insira a senha no campo **Senha antiga**.

7. No grupo de configurações **Aplicar senha a**, especifique as operações com aplicativos cujo acesso está protegido por senha.

8. Clique no botão **Aplicar** na janela **Configurações**.

Uma senha esquecida não pode ser recuperada. Se você esqueceu sua senha, entre em contato com Suporte Técnico para restaurar o acesso às configurações do Kaspersky Internet Security.

PAUSANDO E REINICIANDO A PROTEÇÃO DO COMPUTADOR

Pausar a proteção significa desativar todos os componentes de proteção por um determinado período de tempo.

Para pausar a proteção do computador:

1. No menu de contexto do ícone de aplicativo na área de notificações da barra de tarefas, selecione o item **Pausar proteção**.

   A janela **Pausar proteção** é exibida (consulte a figura abaixo).

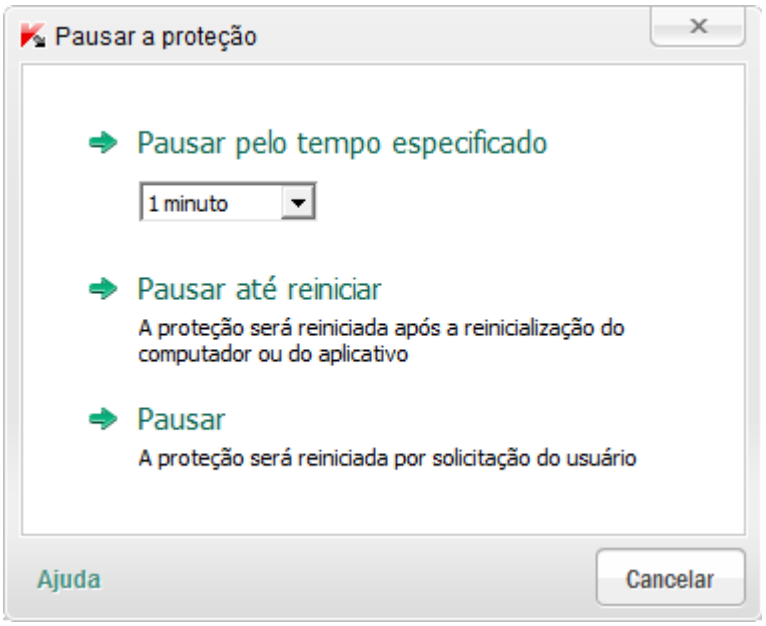

*Figura 8. Janela **Pausar proteção***

2. Na janela **Pausar a proteção**, selecione o intervalo de tempo depois do qual a proteção deve ser reiniciada:

   - **Pausar pelo tempo especificado** – a proteção será ativada quando o intervalo de tempo selecionado na lista suspensa abaixo expirar.
   - **Pausar até reiniciar** – a proteção será ativada depois que o aplicativo ou o sistema operacional forem reiniciados (desde que a execução automática do aplicativo esteja ativada).
   - **Pausar** – a proteção será retomada quando você decidir reiniciá-la.

Para reiniciar a proteção do computador,

selecione o item **Reiniciar a proteção** no menu de contexto do ícone do aplicativo na área de notificações da barra de tarefas.

EXIBINDO O RELATÓRIO DE OPERAÇÃO DO APLICATIVO

O Kaspersky Internet Security mantém relatórios de funcionamento para cada um dos componentes da proteção. Nos relatórios, você pode obter informações estatísticas de operação do aplicativo (por exemplo, saber quantos objetos maliciosos foram detectados e neutralizados em um período especificado, quantas vezes o aplicativo foi atualizado no mesmo período, quantos spams foram detectados e muito mais).

Ao trabalhar em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você pode abrir relatórios usando o Kaspersky Gadget. Para fazer isso, o Kaspersky Gadget deve estar configurado de forma que a opção de abrir a janela de relatórios seja atribuída a um de seus botões (consulte a seção "Usando o Kaspersky Gadget" na página 58).

Para exibir o relatório de operação do aplicativo:

1. Abra a janela **Relatórios** usando um dos seguintes métodos:

   - clique no botão **Relatórios** na parte superior da janela principal do aplicativo;
   - clique no botão com o ícone **Configurações** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).

   Os relatórios de funcionamento do aplicativo são exibidos como gráficos na janela **Relatórios**.

2. Se desejar exibir um relatório detalhado de atividade do aplicativo (por exemplo, um relatório da atividade de cada componente), clique no botão **Relatório detalhado** na parte inferior da janela **Relatório**.

   A janela **Relatório detalhado** será aberta com os dados representados em uma tabela. Para obter uma exibição conveniente dos relatórios, é possível selecionar várias opções de classificação das entradas.

RESTAURAR AS CONFIGURAÇÕES PADRÃO DO APLICATIVO

Você pode restaurar as configurações padrão do Kaspersky Internet Security recomendadas pela Kaspersky Lab a qualquer momento. As configurações podem ser restauradas usando o *Assistente de Configuração do Aplicativo*.

Quando o Assistente concluir sua operação, o nível de segurança *Recomendado* estará definido para todos os componentes de proteção. Ao restaurar o nível de segurança recomendado, você pode salvar os valores especificados anteriormente para algumas das configurações dos componentes do aplicativo.

Para iniciar o Assistente de Solução de Problemas pós-infecção do Microsoft Windows:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, execute o Assistente de Configuração do Aplicativo de uma das seguintes maneiras:

   - clique no link **Restaurar** no canto inferior da janela;

- na parte superior da janela, selecione a seção **Adicional**, subseção **Gerenciar Configurações**, e clique no botão **Restaurar** na seção **Restaurar configurações padrão** (consulte a figura abaixo)

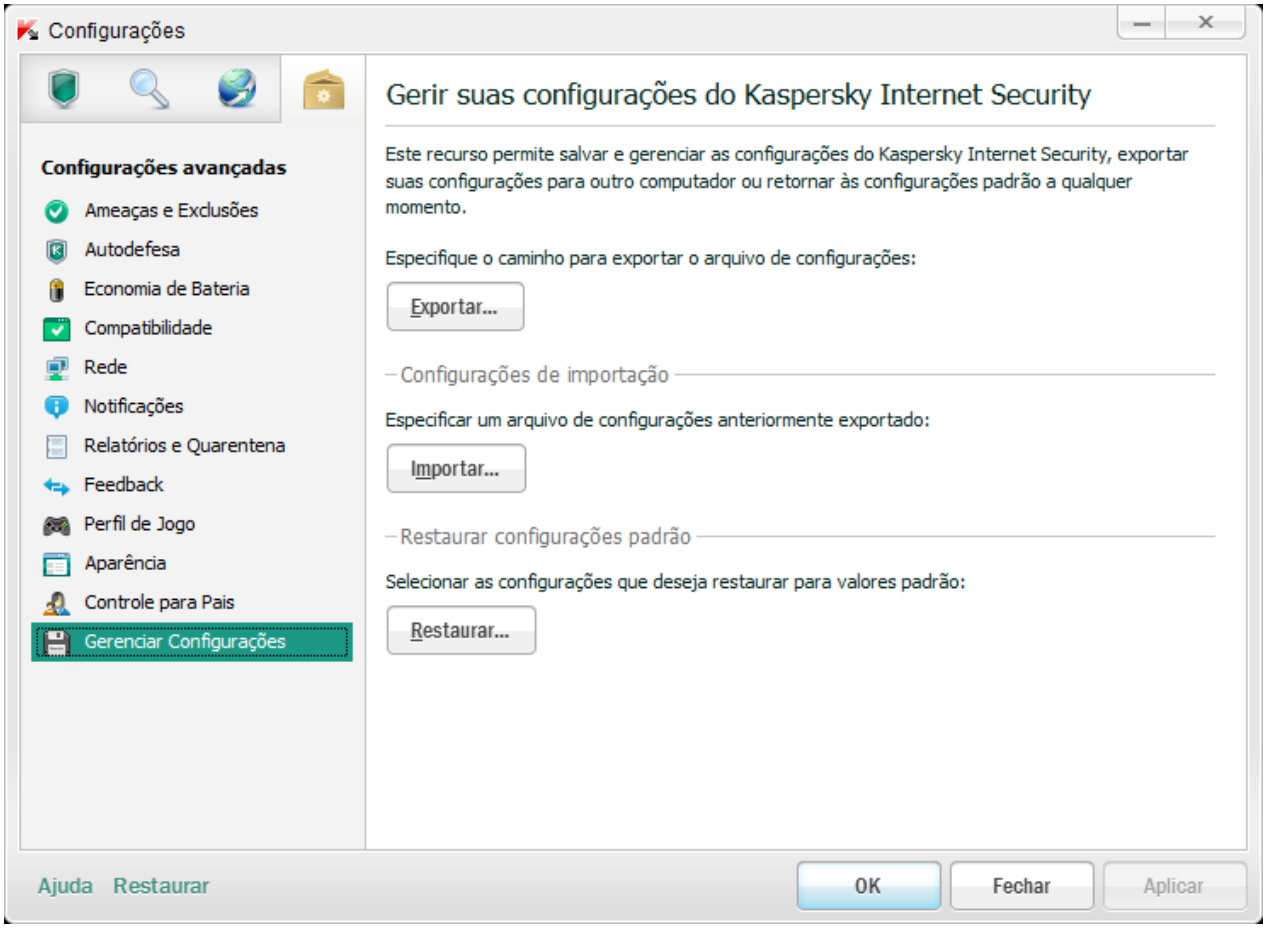

*Figura 9. Janela **Configurações**, subseção **Gerenciar Configurações***

Vamos revisar as etapas do Assistente mais detalhadamente.

Step 1. Iniciando o Assistente

Clique no botão **Avançar** para continuar com o Assistente.

Step 2. Restaurar configurações

Esta janela do Assistente mostra os componentes de proteção do Kaspersky Internet Security cujas configurações são diferentes dos valores padrão porque foram alteradas pelo usuário ou acumuladas pelo treinamento do Kaspersky Internet Security (Firewall ou Antispam). Se tiverem sido criadas configurações especiais para algum componente, elas também serão exibidas nessa janela (consulte a figura abaixo).

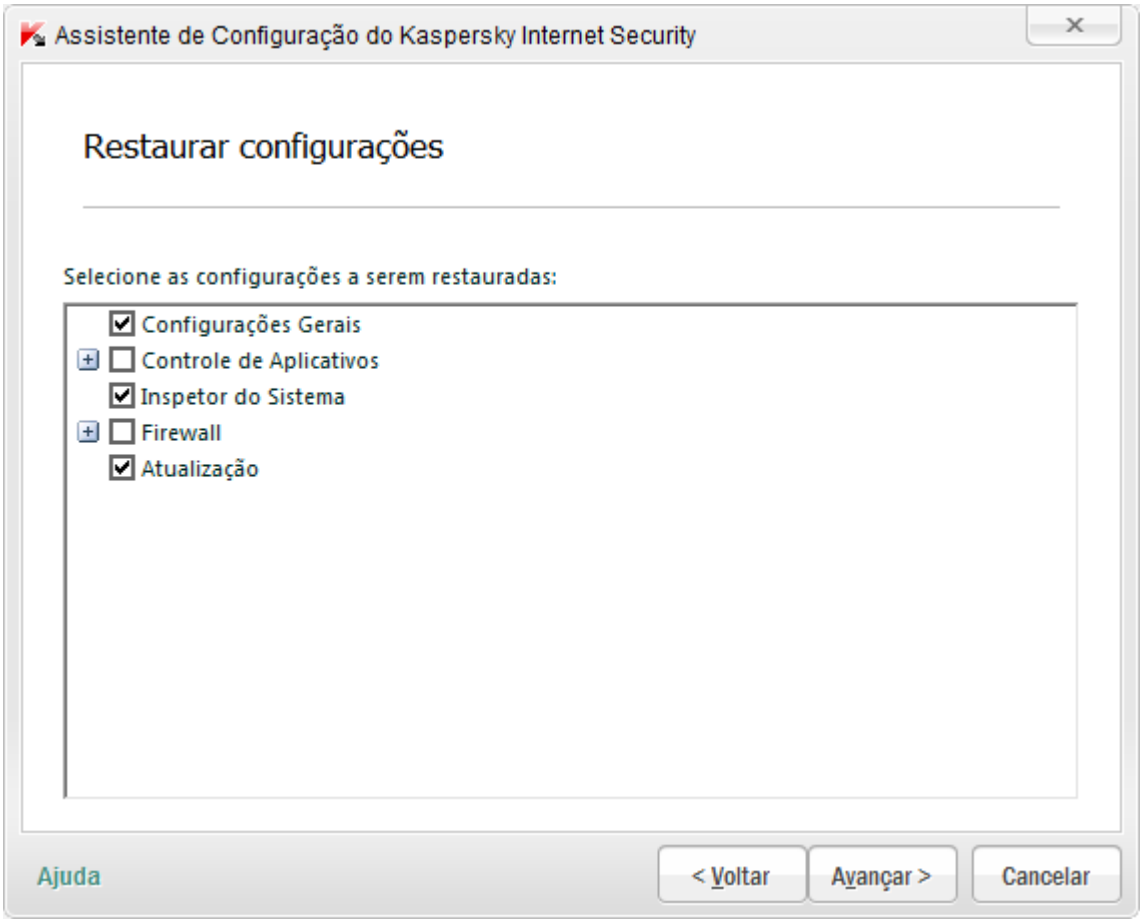

*Figura 10. Janela **Restaurar configurações***

As configurações especiais incluem listas de frases e endereços permitidos e bloqueados usados pelo Antispam, listas de endereços e telefones de provedores confiáveis, regras de exclusão da proteção criadas para componentes do aplicativo e regras de filtragem aplicadas pelo Firewall a pacotes e aplicativos.

As configurações especiais são criadas ao trabalhar com o Kaspersky Internet Security em relação a requisitos de segurança e tarefas individuais. A Kaspersky Lab recomenda salvar suas configurações especiais ao restaurar as configurações padrão do aplicativo.

Marque as caixas correspondentes às configurações que você deseja salvar e clique no botão **Avançar**.

Step 3. Análise do sistema

Nesta etapa, são coletadas informações sobre os aplicativos do Microsoft Windows. Esses aplicativos são adicionados à lista de aplicativos confiáveis que não têm restrições sobre as ações que executam no sistema.

Quando a análise for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 4. Concluindo a restauração

Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**.

IMPORTANDO AS CONFIGURAÇÕES DO APLICATIVO PARA O KASPERSKY INTERNET SECURITY INSTALADO EM OUTRO COMPUTADOR

Depois de configurar o produto, você poderá aplicar suas configurações ao Kaspersky Internet Security instalado em outro computador. Assim, o aplicativo será configurado da mesma maneira nos dois computadores. Esse recurso é útil quando, por exemplo, o Kaspersky Internet Security é instalado no seu computador doméstico e no seu escritório.

As configurações do Kaspersky Internet Security podem ser transferidas para outro computador em três etapas:

1. Exportando as configurações do aplicativo em um arquivo de configuração.
2. Transferindo um arquivo de configuração para outro computador (por exemplo, por email ou em uma mídia removível).
3. Aplicando as configurações de um arquivo de configuração ao aplicativo instalado em outro computador.

Para salvar as configurações do Kaspersky Internet Security em um arquivo de configuração:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na parte superior da janela **Configurações**, na seção **Adicionais**, selecione a subseção **Gerenciar Configurações**.
4. Clique no botão **Exportar** na subseção **Gerenciar Configurações**.
5. Na janela que é aberta, insira o nome do arquivo de configuração e especifique a localização na qual ele deve ser salvo.
6. Clique em **OK**.

Para aplicar as configurações do arquivo de configuração ao aplicativo instalado em outro computador:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na parte superior da janela **Configurações**, na seção **Adicionais**, selecione a subseção **Gerenciar Configurações**.
4. Clique no botão **Importar** na subseção **Gerenciar Configurações**.
5. Na janela que é aberta, selecione o arquivo do qual você deseja importar as configurações do Kaspersky Internet Security.
6. Clique em **OK**.

USANDO O KASPERSKY GADGET

Ao usar o Kaspersky Internet Security em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*). Depois de instalar o Kaspersky Internet Security em um computador com o Microsoft Windows 7, o gadget é exibido automaticamente na área de trabalho. Depois de instalar o aplicativo em um computador com o Microsoft Windows Vista, você deverá adicionar o gadget manualmente à Barra Lateral do Microsoft Windows (consulte a documentação do sistema operacional).

O indicador colorido do gadget exibe o status de proteção do computador da mesma forma que o indicador na janela principal do aplicativo (consulte a seção "Avaliando o status de proteção do computador e solucionando problemas de segurança" na página 29). O verde indica que o computador está totalmente protegido, o amarelo indica que há problemas com a proteção e o vermelho indica que a segurança do computador está em risco. A cor cinza indica que o aplicativo foi interrompido.

Você pode usar o gadget para executar as seguintes ações:

- reiniciar o aplicativo, caso ele tenha sido pausado anteriormente;
- abrir a janela principal do aplicativo;
- verificar objetos especificados quanto à presença de vírus;
- abrir a janela de notícias.

Além disso, você pode configurar os botões do gadget de forma que eles possam executar ações adicionais:

- executar uma atualização;
- editar as configurações do aplicativo;
- exibir os relatórios do aplicativo;
- exibir relatórios do Controle para Pais;
- exibir informações sobre a atividade de rede (Monitor de Rede) e a atividade de aplicativos;
- pausar a proteção;
- abrir o Teclado Virtual;
- abrir a janela do Gerenciador de Tarefas.

Para executar o aplicativo usando o gadget,

clique no ícone **Ativar** localizado no centro do gadget.

Para abrir a janela principal do aplicativo usando o gadget,

clique no ícone do monitor na área central do gadget.

Para verificar um objeto quanto à presença de vírus usando o gadget,

arraste o objeto a ser verificado para o gadget.

O andamento da tarefa será exibido na janela do **Gerenciador de Tarefas**.

Para abrir a janela de notícias usando o gadget,

clique no ícone exibido no centro do gadget quando forem lançadas notícias.

Para configurar o gadget:

1. Abra a janela de configurações do gadget clicando no ícone exibido no canto superior direito do bloco do gadget se você passar o cursor sobre ele.
2. Nas listas suspensas correspondentes aos botões do gadget, selecione as ações que devem ser executadas quando você clicar nesses botões.
3. Clique em **OK**.

A PARTICIPAÇÃO NA KASPERSKY SECURITY NETWORK (KSN)

Para aumentar a eficiência da proteção do computador, o Kaspersky Internet Security usa dados recebidos de usuários de todo o mundo. A Kaspersky Security Network foi criada para coletar esses dados.

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados da Kaspersky Security Network garante um tempo de resposta menor do Kaspersky Internet Security ao encontrar novos tipos de ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Graças aos usuários que participam da Kaspersky Security Network, a Kaspersky Lab consegue coletar informações sobre tipos e fontes de novas ameaças, desenvolver soluções para as neutralizar e minimizar o número de falsos positivos. A participação da Kaspersky Security Network permite acessar estatísticas de reputação para aplicativos e sites.

NESTA SEÇÃO

Ativando e desativando a participação no Kaspersky Security Network 60

Verificando a conexão com o Kaspersky Security Network..... 61

ATIVANDO E DESATIVANDO A PARTICIPAÇÃO NO KASPERSKY SECURITY NETWORK

A participação no Kaspersky Security Network é voluntária. Você pode ativar ou desativar o uso do Kaspersky Security Network ao instalar o Kaspersky Internet Security e/ou em qualquer momento após a instalação do aplicativo.

Para ativar e desativar a participação no Kaspersky Security Network:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Configurações**.
3. Na janela **Configurações** que é exibida, na seção **Configurações Avançadas**, selecione a subseção **Feedback**.
4. No lado direito da janela, execute uma das seguintes ações:
   - Se desejar participar no KSN, selecione a caixa de seleção **Eu concordo em participar do programa Kaspersky Security Network**.
   - Se não desejar participar no KSN, desmarque a caixa de seleção **Eu concordo em participar do programa Kaspersky Security Network**.

VERIFICANDO A CONEXÃO COM A KASPERSKY SECURITY NETWORK

A conexão com a Kaspersky Security Network pode ser perdida devido aos seguintes motivos:

- Você não participa da Kaspersky Security Network.
- Seu computador não está conectado à Internet.
- O status da chave atual não permite conexão com a Kaspersky Security Network.

O status da chave atual é exibido na janela **Licença** (consulte a seção "**Comprando e renovando uma licença**" na página 28).

Para testar a conexão com a Kaspersky Security Network:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no botão **Proteção em nuvem**.

   À esquerda da janela que é aberta, é exibido o status de conexão com o Kaspersky Security Network.

ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO

Esta seção fornece informações sobre como obter suporte técnico e os requisitos para receber ajuda do Suporte Técnico.

NESTA SEÇÃO

Como obter suporte técnico 62

Suporte técnico por telefone 62

Obtendo suporte técnico através da Minha conta Kaspersky 63

Usando o arquivo de rastreamento e o script do AVZ 64

COMO OBTER SUPORTE TÉCNICO

Se você não encontrar uma solução para seu problema na documentação do aplicativo ou em uma das fontes de informações sobre o aplicativo (consulte a seção "Fontes de informações sobre o aplicativo" na página 9), é recomendável entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab. Os especialistas do Serviço de Suporte Técnico responderão todas as suas dúvidas sobre a instalação e o uso do aplicativo.

Antes de entrar em contato com o Suporte Técnico, leia as regras de suporte (http://support.kaspersky.com/support/rules).

Você pode entrar em contato com o Serviço de Suporte Técnico de uma das seguintes maneiras:

- Por telefone. Este método permite consultar especialistas do nosso Suporte Técnico em russo ou internacional.
- Enviando uma consulta da Minha conta Kaspersky no site do Serviço de Suporte Técnico. Este método permite o contato com nossos especialistas usando o formulário de consulta.

O Suporte Técnico está disponível somente para usuários que compraram a licença comercial. Não é fornecido qualquer suporte a usuários das versões de avaliação.

SUPORTE TÉCNICO POR TELEFONE

Se ocorrer um problema urgente, você poderá ligar para os especialistas do Suporte Técnico em russo ou internacional (http://support.kaspersky.com/support/international) por telefone.

Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte (http://support.kaspersky.com/support/details). Assim, nossos especialistas poderão ajudá-lo mais rapidamente.

OBTENDO SUPORTE TÉCNICO ATRAVÉS DA MINHA CONTA KASPERSKY

Minha conta Kaspersky é sua área pessoal (https://my.kaspersky.com) no site do Serviço de Suporte Técnico.

Para obter acesso à Minha conta Kaspersky, execute o procedimento de registro na página de registro (https://my.kaspersky.com/registration). Insira seu endereço de email e uma senha para entrar na Minha conta Kaspersky.

Na Minha conta Kaspersky, você pode executar as seguintes ações:

- Entrar em contato com o Suporte Técnico e o Laboratório de Vírus.
- Entrar em contato com o Suporte Técnico sem usar o email.
- Rastrear o status das suas solicitações em tempo real.
- Exibir um histórico detalhado de suas solicitações do Suporte Técnico.
- Receber uma cópia do arquivo de chave, caso ele tenha sido perdido ou removido.

Suporte técnico por email

Você pode enviar uma solicitação online para o Suporte Técnico em inglês, russo, alemão, francês ou espanhol.

Nos campos do formulário de solicitação online, especifique os seguintes dados:

- Tipo de solicitação
- Nome do aplicativo e número da versão
- Descrição da solicitação
- ID do cliente e senha
- Endereço de email

Um especialista do Serviço de Suporte Técnico envia uma resposta à sua pergunta para a Minha conta Kaspersky e para o endereço de email especificado na solicitação online.

Solicitação online para o Laboratório de Vírus

Algumas solicitações devem ser enviadas para o Laboratório de Vírus e não para o Suporte Técnico.

Você pode enviar os seguintes tipos de solicitações para o Laboratório de Vírus:

- *Programa malicioso desconhecido* – você suspeita que um arquivo contém um vírus, mas o Kaspersky Internet Security não o identificou como infectado.

  Os especialistas do Laboratório de Vírus analisam o código malicioso enviado. Se detectarem um vírus desconhecido, eles adicionarão uma descrição correspondente ao banco de dados, que se tornará disponível ao atualizar os aplicativos antivírus.

- *Falso positivo* – o Kaspersky Internet Security classifica um arquivo como vírus, mas você tem certeza de que o arquivo não é um vírus.

- *Solicitação de descrição de programa malicioso* – você deseja receber a descrição de um vírus detectado pelo Kaspersky Internet Security usando o nome do vírus.

Também é possível enviar solicitações ao Laboratório de Vírus da página com o formulário de solicitação (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt) sem estar registrado na Minha conta Kaspersky. Nessa página, não é necessário especificar o código de ativação do aplicativo.

USANDO O ARQUIVO DE RASTREAMENTO E O SCRIPT DO AVZ

Depois de notificar os especialistas do Serviço de Suporte Técnico sobre um problema ocorrido, eles podem solicitar que você crie um relatório com informações sobre o sistema operacional e o envie para o Serviço de Suporte Técnico. Além disso, os especialistas do Serviço de Suporte Técnico podem solicitar que você crie um *arquivo de rastreamento*. O arquivo de rastreamento permite rastrear o processo de realizar comandos do aplicativo, passo a passo, e determinar a etapa da operação do aplicativo em que o erro ocorre.

Depois que os especialistas do Serviço de Suporte Técnico analisarem os dados que você enviar, eles poderão criar um script do AVZ e enviá-lo para você. Ao executar os scripts do AVZ, você pode analisar os processos ativos e verificar o sistema quanto à presença de código malicioso, desinfetar/excluir arquivos infectados e criar relatórios com os resultados das verificações do sistema.

NESTA SEÇÃO

Criando um relatório de estado do sistema 64

Enviando arquivos de dados 65

Execução do script do AVZ 66

CRIANDO UM RELATÓRIO DE ESTADO DO SISTEMA

Para criar um relatório de estado do sistema:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela que é aberta, clique no botão **Ferramentas de Suporte**.

   A janela **Ferramentas de Suporte** é exibida.
4. Na janela que é aberta, clique no botão **Criar relatório de estado do sistema**.

O relatório de estado do sistema é criado nos formatos HTML e XML e é salvo no arquivo comprimido sysinfo.zip. Quando as informações sobre o sistema forem coletadas, você poderá exibir o relatório.

Para exibir o relatório:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela que é aberta, clique no botão **Ferramentas de Suporte**.

   A janela **Ferramentas de Suporte** é exibida.
4. Na janela que é aberta, clique no link **Exibir relatório**.

   A janela do Microsoft Windows Explorer é aberta.
5. Na janela exibida, abra o arquivo com o nome sysinfo.zip que contém arquivos de relatório.

ENVIANDO ARQUIVOS DE DADOS

Depois de criar os arquivos de rastreamento e o relatório de estado do sistema, você deverá enviá-los aos especialistas do Serviço de Suporte Técnico da Kaspersky Lab.

Você precisará de um número de solicitação para carregar os arquivos no servidor do Serviço de Suporte Técnico (consulte a seção "Obtendo suporte técnico através da Minha conta Kaspersky" na página 63). Esse número estará disponível na sua Minha conta Kaspersky no site do Serviço Suporte Técnico, se a sua solicitação estiver ativa.

Para carregar os arquivos de dados no servidor do Serviço de Suporte Técnico:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela que é aberta, clique no botão **Ferramentas de Suporte**.

   A janela **Ferramentas de Suporte** é exibida.
4. Na janela exibida, clique no botão **Enviar dados de serviço para o Suporte Técnico**.

   A janela **Enviar relatório** é aberta.
5. Selecione as caixas ao lado dos dados que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   A janela **Inserir número de solicitação** é aberta.
6. Especifique o número atribuído à sua solicitação entrando em contato com o Serviço de Suporte Técnico através da Minha Conta Kaspersky e clique no botão **OK**.

Os arquivos de dados selecionados são compactados e enviados ao servidor do Serviço de Suporte Técnico.

Se, por algum motivo, não for possível entrar em contato com o Serviço de Suporte Técnico, os arquivos de dados poderão ser armazenados no seu computador e enviados posteriormente a partir da Minha conta Kaspersky.

Para salvar os arquivos de dados em disco:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela que é aberta, clique no botão **Ferramentas de Suporte**.
4. A janela **Ferramentas de Suporte** é exibida.
5. Na janela exibida, clique no botão **Enviar dados de serviço para o Suporte Técnico**.

   A janela **Enviar relatório** é aberta.
6. Selecione as caixas ao lado dos dados que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   A janela **Inserir número de solicitação** é aberta.
7. Clique no botão **Cancelar** e, na janela que é aberta, confirme a gravação dos arquivos em disco clicando no botão **Sim**.

   A janela para gravação do arquivo comprimido será aberta.
8. Especifique o nome do arquivo comprimido e confirme a gravação.

O arquivo comprimido criado pode ser enviado ao Serviço de Suporte Técnico a partir da Minha conta Kaspersky.

EXECUÇÃO DO SCRIPT DO AVZ

Não é recomendável alterar o texto de um script do AVZ recebido dos especialistas da Kaspersky Lab. Se ocorrerem problemas durante a execução, entre em contato com o Serviço de Suporte Técnico (consulte a seção "Como obter suporte técnico" na página 62).

Para executar o script do AVZ:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela que é aberta, clique no botão **Ferramentas de Suporte**.

   A janela **Ferramentas de Suporte** é exibida.
4. Na janela que é aberta, clique no botão **Executar script**.

   A janela **Execução do script do AVZ** é exibida.
5. Copie o texto do script enviado pelos especialistas do Serviço de Suporte Técnico, cole no campo de inserção de dados na janela exibida e clique no botão **Avançar**.

   O script é executado.

Se o script for executado com êxito, o Assistente será automaticamente fechado. Se ocorrer um erro durante a execução do script, o Assistente exibirá uma mensagem correspondente.

GLOSSÁRIO

A

ANALISADOR HEURÍSTICO

Uma tecnologia de detecção de informações sobre ameaças que ainda não foram adicionadas aos bancos de dados da Kaspersky Lab. O analisador heurístico permite detectar objetos com um comportamento no sistema semelhante ao comportamento típico de ameaças. Os objetos detectados pelo analisador heurístico são considerados provavelmente infetados. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

APLICATIVO INCOMPATÍVEL

Aplicativo antivírus de outro desenvolvedor ou aplicativo da Kaspersky Lab que não dá suporte ao gerenciamento por meio do Kaspersky Internet Security.

ARQUIVO COMPRIMIDO

Um ou vários arquivos compactados num único arquivo através da compactação. É necessário um arquivo do aplicativo dedicado e comprimido, para compactar e descompactar dados.

ARQUIVO COMPACTADO

Um arquivo comprimido que contém um programa de descompactação e instruções para sua execução pelo sistema operacional.

ASSINATURA DIGITAL

Um bloco criptografado de dados incorporado em um documento ou aplicativo. É usada uma assinatura digital para identificar o autor do documento ou aplicativo. Para criar uma assinatura digital, o autor do documento ou aplicativo deve ter um certificado digital que prove a sua identidade.

Uma assinatura digital permite verificar a origem e a integridade dos dados e fornece proteção contra falsificações.

ATIVANDO O APLICATIVO

Alterna o aplicativo para o modo totalmente funcional. A ativação do aplicativo é efetuada pelo usuário durante ou após a instalação do aplicativo. O usuário deve ter um código de ativação para ativar o aplicativo.

ATUALIZAÇÃO

Procedimento de substituição/adição de novos arquivos (bancos de dados ou módulos do aplicativo) recuperados dos servidores de atualização da Kaspersky Lab.

ATUALIZAÇÃO DISPONÍVEL

Um conjunto de atualizações dos módulos do aplicativo da Kaspersky Lab que inclui as atualizações críticas acumuladas por um determinado período e as alterações da arquitetura do aplicativo.

B

BANCOS DE DADOS

Bancos de dados que contêm descrições das ameaças de segurança para o computador conhecidas pela Kaspersky Lab no momento de publicação dos bancos de dados. Os registros que são incluídos nos bancos de dados permitem a detecção de código malicioso em objetos verificados. Os bancos de dados são criados pelos peritos da Kaspersky Lab e atualizados a cada hora.

BANCO DE DADOS DE ENDEREÇOS MALICIOSOS

Uma lista de endereços da Web cujo conteúdo pode ser considerado perigoso. A lista foi criada pelos especialistas da Kaspersky Lab. Ela é atualizada periodicamente, sendo incluída no pacote do aplicativo da Kaspersky Lab.

BANCO DE DADOS DE ENDEREÇOS DE PHISHING

Lista de endereços da Web definidos pelos especialistas da Kaspersky Lab como endereços de phishing. O banco de dados é atualizado periodicamente e faz parte do aplicativo da Kaspersky Lab.

BLOQUEIO DE UM OBJETO

Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído.

C

CÓDIGO DE ATIVAÇÃO

Um código que você recebe ao comprar a licença comercial do Kaspersky Internet Security. Esse código é necessário para a ativação do aplicativo.

O código de ativação é uma sequência exclusiva de vinte caracteres alfanuméricos no formato xxxxx-xxxxx-xxxxx-xxxxx.

COMPONENTES DE PROTEÇÃO

Partes integrais do Kaspersky Internet Security que se destinam à proteção contra tipos específicos de ameaças (por exemplo, Antispam e Antiphishing). Cada um dos componentes é relativamente independente dos restantes, por isso pode ser desativado ou configurado individualmente.

CONFIGURAÇÕES DA TAREFA

Configurações do aplicativo que são específicas de cada tipo de tarefa.

CONFIGURAÇÕES DO APLICATIVO

Configurações do aplicativo que são comuns a todos os tipos de tarefa, regulando a operação do aplicativo como um todo, como as configurações de desempenho do aplicativo, as configurações de relatórios e as configurações da Quarentena.

CLASSIFICAÇÃO DE AMEAÇA

Um índice que exibe a probabilidade do risco de ameaça de um aplicativo para o sistema operacional. A classificação de ameaça é calculada usando a análise heurística com base em dois tipos de critérios:

- estáticos (como as informações sobre o arquivo executável de um aplicativo: tamanho, data de criação, etc.);
- dinâmicos, que são usados ao simular a operação do aplicativo em um ambiente virtual (análise das solicitações de funções do sistema pelo aplicativo).

A classificação de ameaça permite detectar o comportamento típico de malware. Quando menor for a classificação de ameaça, o aplicativo terá permissão de executar mais ações no sistema.

E

EXCLUSÃO

Uma exclusão é um objeto excluído da verificação pelo aplicativo da Kaspersky Lab. Você pode excluir da verificação arquivos de determinados formatos, máscaras de arquivos, uma determinada área (por exemplo, uma pasta ou um programa), processos de aplicativos ou objetos por tipo de ameaça, de acordo com a classificação da Enciclopédia de Vírus. A cada tarefa pode ser atribuído um conjunto de exclusões.

EXCLUSÃO DE MENSAGENS

O método de processamento de um email, no qual a mensagem é removida fisicamente. É recomendável aplicar este método às mensagens que certamente contêm spam ou malware. Antes de excluir uma mensagem, uma cópia da mesma é salva na Quarentena (a menos que essa opção esteja desativada).

EXCLUSÃO DE UM OBJETO

Método de processamento de objetos que os exclui fisicamente de seu local original (disco rígido, pasta, recurso de rede). É recomendável aplicar esse método a objetos perigosos que, por algum motivo, não podem ser desinfetados.

F

FALSO POSITIVO

Uma situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido à semelhança de seu código com o de um vírus.

K

KASPERSKY SECURITY NETWORK (KSN)

Uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados da Kaspersky Security Network garante um tempo de resposta menor de aplicativos da Kaspersky Lab ao encontrar novos tipos de ameaças, melhora a eficiência de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

KEYLOGGER

Um programa concebido para registro oculto de informações sobre as teclas pressionadas pelo usuário. Os keyloggers são também chamados de interceptores ou espiões de teclas.

M

MÁSCARA DE ARQUIVOS

Representação de um nome de arquivo usando curingas. Os curingas padrão usados em máscaras de arquivos são * e ?, onde * representa qualquer número de caracteres e ? representa qualquer caractere.

MÓDULOS DO APLICATIVO

Arquivos fornecidos no pacote de instalação da Kaspersky Lab, responsáveis pela execução de suas principais tarefas. Um módulo executável específico corresponde a cada tipo de tarefa executada pelo aplicativo (proteção em tempo real, verificação por demanda, atualizações). Ao executar uma verificação completa do computador na janela principal, você inicia a execução do módulo dessa tarefa.

N

NÍVEL DE SEGURANÇA

O nível de segurança é definido como uma coleção de configurações predefinida para um componente do aplicativo.

O

OBJETO INFECTADO

Um objeto que inclui uma seção cujo código completo corresponde a uma seção de uma ameaça conhecida. A Kaspersky Lab não recomenda usar estes objetos.

OBJETO PROVAVELMENTE INFETADO

Um objeto cujo código contém código modificado de uma ameaça ou código conhecido, o qual é semelhante ao de uma ameaça, consoante seu comportamento.

OBJETO QUE PODE SER INFETADO

Um objeto que, devido à sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e distribuir código malicioso. Normalmente, são arquivos executáveis, por exemplo, arquivos com as extensões COM, EXE, DLL, etc. O risco de infiltração de código malicioso nesses arquivos é bastante alto.

OBJETOS DE INICIALIZAÇÃO

Conjunto de programas necessários para iniciar e operar corretamente o sistema operacional e os softwares instalados no computador. Esses objetos são executados sempre que o sistema operacional é iniciado. Existem vírus capazes de infectar esses objetos de forma específica, o que pode levar, por exemplo, ao bloqueio da inicialização do sistema operacional.

P

PACOTE DE ATUALIZAÇÃO

Um pacote de arquivos para atualizar módulos do aplicativo. Um aplicativo da Kaspersky Lab copia os pacotes de atualizações dos servidores de atualizações da Kaspersky Lab e os instala e aplica automaticamente.

PHISHING

Um tipo de fraude na Internet, em que as mensagens de email são enviadas com o propósito de roubar informações confidenciais. Normalmente, estas informações são relacionadas com dados financeiros.

PROCESSO CONFIÁVEL

O processo de um programa cujas operações com arquivos não são monitoradas pelo aplicativo da Kaspersky Lab no modo de proteção em tempo real. Ao detectar uma atividade suspeita de um processo confiável, o Kaspersky Internet Security excluir o processo da lista de processos confiáveis e bloqueia todas as suas atividades.

PROTOCOLO

Um conjunto de regras claramente definido e padronizado que define a interação entre um cliente e um servidor. Protocolos conhecidos e os serviços associados a eles incluem o HTTP, o FTP e o NNTP.

Q

QUARENTENA

Um armazenamento dedicado onde o aplicativo coloca cópias de backup dos arquivos que foram modificados ou excluídos durante a desinfecção. As cópias de arquivos são armazenadas em um formato especial e não representam qualquer ameaça para o computador.

R

RASTROS

Execução do aplicativo no modo de depuração; depois que cada comando é executado, o aplicativo é interrompido e o resultado da etapa é exibido.

ROOTKIT

Um programa ou um conjunto de programas desenvolvidos para ocultar rastros de um invasor ou um malware no sistema operacional.

Em sistemas operacionais baseados em Windows, um rootkit normalmente significa um programa que invade o sistema operacional e intercepta suas funções (APIs do Windows). Acima de tudo, a interceptação e modificação de funções de APIs de nível inferior permite que esse programa mascare sua presença no sistema. Um rootkit pode geralmente mascarar a presença de quaisquer processos, pastas e arquivos que estão armazenados em uma unidade de disco, além de chaves de registro, caso sejam descritas na configuração do rootkit. Vários rootkits instalam seus próprios drivers e serviços no sistema operacional (eles também são "invisíveis").

S

SCRIPT

Um pequeno programa de computador ou uma parte independente de um programa (função) que, como regra, foi desenvolvido para executar uma tarefa específica. É usado com mais frequência com programas incorporados no hipertexto. Os scripts são executados, por exemplo, quando você abre sites específicos.

Se a proteção em tempo real estiver ativada, o aplicativo controlará a execução de scripts, os interceptará e verificará a presença de vírus. Dependendo dos resultados da verificação, você poderá bloquear ou permitir a execução do script.

SERVIDORES DE ATUALIZAÇÃO DA KASPERSKY LAB

Os servidores HTTP da Kaspersky Lab para onde o banco de dados de antivírus e os módulos do aplicativo são carregados.

SETOR DE INICIALIZAÇÃO DO DISCO

O setor de inicialização é uma área específica no disco rígido, disquete ou outro dispositivo de armazenamento de dados do computador. Ele contém informações sobre o sistema de arquivos do disco e um programa de carregamento de inicialização responsável por iniciar o sistema operacional.

Existem diversos vírus que infectam os setores de inicialização, os chamados vírus de inicialização. O aplicativo da Kaspersky Lab permite verificar os setores de inicialização quanto à presença de vírus e desinfetá-los, caso seja detectada uma infecção.

SPAM

Mensagens de email não solicitadas enviadas em massa, frequentemente contendo mensagens publicitárias.

SPAM PROVÁVEL

Uma mensagem que não pode ser considerada spam com certeza, mas que apresenta alguns atributos de spam (por exemplo, determinados tipos de correspondência e mensagens publicitárias).

SURTO DE VÍRUS

Uma série de tentativas deliberadas de infectar um computador com vírus.

T

TAREFA

As funções executadas pelo aplicativo da Kaspersky Lab são implementadas como tarefas, como: Proteção em tempo real, Verificação completa do computador, Atualização do banco de dados.

TECNOLOGIA ICHECKER

Uma tecnologia que permite aumentar a velocidade das verificações antivírus por meio da exclusão de objetos que permaneceram inalterados desde a última verificação, desde que os parâmetros de verificação (as configurações e os bancos de dados) não tenham mudado. As informações de cada arquivo são armazenadas em um banco de dados especial. Essa tecnologia é usada nos modos de proteção em tempo real e de verificação por demanda.

Por exemplo, você tem um arquivo comprimido que foi verificado pelo aplicativo da Kaspersky Lab e ao qual foi atribuído o status não infetado. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se você alterou o conteúdo do arquivo comprimido adicionando um novo objeto a ele, se modificou as configurações de verificação ou se atualizou o banco de dados do aplicativo, o arquivo comprimido será verificado novamente.

Limitações da tecnologia iChecker:

- essa tecnologia não funciona com arquivos grandes, pois é mais rápido verificar o arquivo que analisar se ele foi modificado desde sua última verificação;
- a tecnologia oferece suporte a um número limitado de formatos.

TERMO DA LICENÇA

O termo da licença é um período de tempo durante o qual você tem acesso aos recursos do aplicativo e direitos de uso dos serviços adicionais.

V

VERIFICAÇÃO DO TRÁFEGO

Verificação em tempo real dos objetos transferidos por todos os protocolos (por exemplo, HTTP, FTP, etc.) que usa informações da versão atual (mais recente) dos bancos de dados.

VÍRUS

Um programa que infeta outros programas adicionando o seu código para obter controle dos arquivos infetados quanto estes são executados. Esta definição simples permite expor a principal ação realizada por qualquer vírus – infecção.

VÍRUS DESCONHECIDO

Um novo vírus sobre o qual não há informações nos bancos de dados. Em geral, os vírus desconhecidos são detectados pelo aplicativo em objetos usando o analisador heurístico e esses objetos são classificados como provavelmente infetados.

VULNERABILIDADE

Uma falha em um sistema operacional ou um aplicativo que pode ser explorada por criadores de software malicioso para invadir o sistema ou o aplicativo e corromper sua integridade. Um elevado número de vulnerabilidades em um sistema torna-o não confiável, uma vez que os vírus que invadiram o sistema podem causar falhas de funcionamento no sistema e nos aplicativos instalados.

KASPERSKY LAB ZAO

O software da Kaspersky Lab é conhecido internacionalmente por sua proteção contra vírus, malware, spam, ataques de rede e de hackers, além de outras ameaças.

Em 2008, a Kaspersky Lab foi classificada como um dos quatro principais fornecedores de soluções de software de segurança de informações para o usuário final (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é o desenvolvedor de sistemas de proteção de computadores preferido dos usuários domésticos na Rússia, de acordo com a pesquisa da "TGI-Russia 2009".

A Kaspersky Lab foi fundada na Rússia em 1997. Atualmente, é um grupo internacional de empresas sediado em Moscou, com cinco divisões regionais que gerenciam as atividades da empresa na Rússia, na Europa Ocidental e Oriental, no Oriente Médio, na África, nas Américas do Norte e do Sul, no Japão, na China e em outros países da região do Pacífico Asiático. A empresa emprega mais de 2.000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab oferecem proteção para todos os tipos de sistemas: de computadores domésticos a grandes redes corporativas.

A linha de produtos pessoais inclui aplicativos antivírus para computadores desktop, laptop e portáteis, além de smartphones e outros dispositivos móveis.

A Kaspersky Lab fornece aplicativos e serviços para proteger estações de trabalho, servidores de arquivos e de email, gateways de email e firewalls. Usadas em conjunto com o sistema de gerenciamento centralizado da Kaspersky Lab, essas soluções garantem a proteção automatizada eficiente de empresas e organizações contra as ameaças de computadores. Os produtos da Kaspersky Lab são certificados pelos principais laboratórios de testes, são compatíveis com os softwares de diversos fornecedores de aplicativos para computadores e são otimizados para a execução em várias plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham 24 horas por dia. Todos os dias, eles descobrem centenas de novas ameaças de computador, criam ferramentas para detectá-las e desinfetá-las, e as incluem nos bancos de dados usados pelos aplicativos da Kaspersky Lab. *O banco de dados do antivírus da Kaspersky Lab é atualizado a cada hora* e o *banco de dados do antispam*, *a cada cinco minutos*.

Tecnologias. Várias tecnologias que agora são parte integrante de modernas ferramentas antivírus foram originalmente desenvolvidas pela Kaspersky Lab. Portanto, faz sentido o fato de que diversos outros desenvolvedores de software usam o kernel do Kaspersky Anti-Virus em seus próprios aplicativos. Essas empresas incluem a SafeNet (EUA), Alt-N Technologies (EUA), Blue Coat Systems (EUA), Check Point Software Technologies (Israel), Clearswift (Reino Unido), CommuniGate Systems (EUA), Critical Path (Irlanda), D-Link (Taiwan), M86 Security (EUA), GFI (Malta), IBM (EUA), Juniper Networks (EUA), LANDesk (EUA), Microsoft (EUA), NETASQ (França), NETGEAR (EUA), Parallels (Rússia), SonicWALL (EUA), WatchGuard Technologies (EUA), ZyXEL Communications (Taiwan). Muitas das tecnologias inovadoras da empresa são patenteadas.

Realizações. Ao longo dos anos, a Kaspersky Lab recebeu centenas de prêmios por seus serviços no combate às ameaças de computador. Por exemplo, em 2010, o Kaspersky Anti-Virus recebeu vários prêmios Advanced+ em uma série de testes administrados pela AV-Comparatives, um renomado laboratório de antivírus austríaco. Mas a principal realização da Kaspersky Lab é a fidelidade de seus usuários em todo o mundo. Os produtos e as tecnologias da empresa protegem mais de 300 milhões de usuários, e seus clientes corporativos somam mais de 200.000.

Site da Kaspersky Lab:	http://brazil.kaspersky.com
Enciclopédia de Vírus:	http://www.securelist.com
Laboratório de Antivírus:	newvirus@kaspersky.com (somente para o envio de arquivos possivelmente infectados no formato comprimido)
	http://support.kaspersky.com/virlab/helpdesk.html
	(para consultas endereçadas aos analistas de vírus)
Fórum da Kaspersky Lab na Web:	http://forum.kaspersky.com

INFORMAÇÕES SOBRE CÓDIGO DE TERCEIROS

As informações sobre códigos de terceiros estão contidas no arquivo legal_notices.txt, armazenado na pasta de instalação do aplicativo.

AVISOS DE MARCAS REGISTRADAS

As marcas registradas e marcas de serviço são propriedade de seus respectivos proprietários.

Google Chrome é uma marca registrada da Google, Inc.

Intel e Pentium são marcas registradas da Intel Corporation e registradas nos Estados Unidos e outros países.

Microsoft, Windows, Windows Vista e Internet Explorer são marcas registradas da Microsoft Corporation registradas nos Estados Unidos da América e em outros países.

Mozilla e Firefox são marcas registradas da Mozilla Foundation.

ÍNDICE

A

Ameaças de segurança 29
Análise de segurança 29
Antiphishing 40
Antispam 36
Antivírus da Web
  Consultor de URLs Kaspersky 47
  Filtro Geográfico 47
  Navegação Segura 47
Antivírus de Email 35
Aplicativos desconhecidos 36
Ativação do aplicativo
  código de ativação 24
  licença 23
  versão de avaliação 17
Ativando o aplicativo 27
Atualização 30

B

Banco Virtual 44
Bancos de dados do aplicativo 30

C

Chave 23
Código de ativação 24
Componentes do aplicativo 12
Consultor de URLs Kaspersky
  Antivírus da Web 47
Conta de usuário 49
Contrato de Licença do Usuário Final 23
Controle de Aplicativos
  criando uma regra de aplicativo 38
  exclusões 38
  regras de acesso de dispositivos 38
Controle para Pais 48
  ativando e configurando 49
  estatísticas do funcionamento do componente 49

D

Dados confidenciais 39
Diagnóstico 29
Disco de Recuperação 50

E

Email indesejado 36
Estatísticas 55
Exibindo estatísticas 55

F

Ferramentas Adicionais
Disco de Recuperação 50
Limpeza de Dados Particulares 45
Solução de problemas do Microsoft Windows 33
Firewall
criando uma regra de aplicativo 38
Fonte de atualização 30
Funcionamento do aplicativo no modo de tela inteira 50

G

Gadget 58

I

Importar/exportar as configurações 58
INSTALANDO O APLICATIVO 15
Interceptador de teclado
proteção contra interceptação de dados pelo teclado 43
Interceptadores de teclado
Teclado Virtual 40

K

KASPERSKY 73
KASPERSKY LAB 73
Kaspersky Security Network 60

L

Licença 23
código de ativação 24
Contrato de Licença do Usuário Final 23
Log de eventos 55

N

Notificações 28

O

O Kaspersky Gadget 58
Objeto desinfetado 32
Objeto infetado 69

P

Perfil de Jogo 50
Problemas de segurança 29

Q

Quarentena
restaurar um objeto 32

R

Rastreamento
carregando resultados de rastreamento 65
Região do domínio 47
Relatórios 55
Removendo o aplicativo 21

Requisitos de hardware 14
Requisitos de software 14
Restaurando as configurações padrão 55
Restringindo o acesso ao aplicativo 53

S

Solução de problemas do Microsoft Windows 33
Spam 36
Status da proteção 29

T

Teclado Virtual 40

V

Verificação de Vulnerabilidades 36
Vulnerabilidade 36